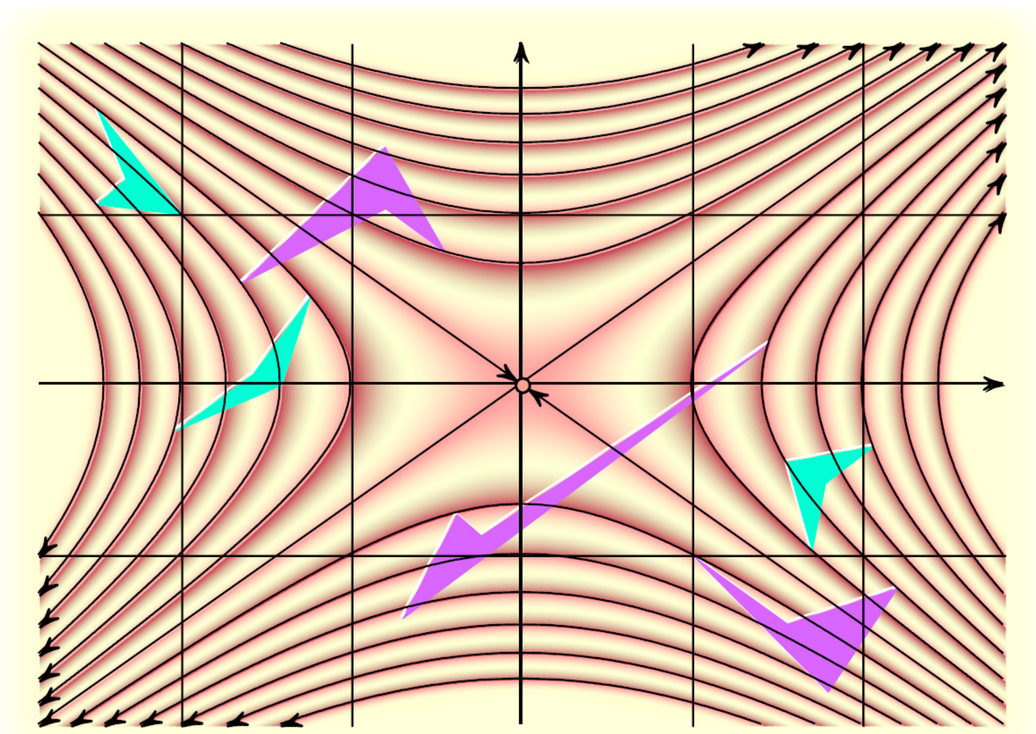
ודים בוגיינקו

תורגם ע"י מריה סבצ'וק

משוואות פֵּל



זהו תרגום מרוסית של הספר:

В.О. Бугаенко. Уравнения Пелля. Второе издание. МЦНМО, 2010.

http://biblio.mccme.ru/node/2342/shop

קובץ PDF של ההוצאה הראשונה ברוסית:

http://www.mccme.ru/mmmf-lectures/books/books/book.13.pdf

משוואות דיאופנטיות

בתחומים שונים של מתמטיקה, במיוחד בגיאומטריה אלגברית ובתורת מספרים, אנחנו פוגשים משוואות ששני אגפים שלהן מהווים פולינומים, והפתרון אמור להיות מספר שלם. משוואות כאלה נקראות *משוואות דיאופנטיות*. קיימים סוגים של משוואות דיאופנטיות שנפטרים בקלות באמצעות כלים אלמנטריים, ויש כאלה שפתרונם דורשים שימוש בתיאוריות מתמטיות מודרניות. אחת הדוגמאות למשוואות כאלה – המשוואות המפורסמות של פרמא

$$a^n + b^n = z^n, \;\; n > 2$$

שהאנושות ניסתה לפתור במשך יותר משלושה מאות שנים, ורק לפני כמה שנים מתמטיקאי אנגלי אנדרו ויילס הצליח להוכיח שהמשוואות אינן פתירות במספרים שלמים חיוביים.

מהי משוואת פל?

משוואת פֶל היא משוואה מהצורה

$$x^2 - my^2 = 1 \tag{1}$$

כאשר m הוא מספר טבעי שאינו ריבוע שלם. סוג זה של משוואות דיאופנטיות ריבועיות קשור להרבה בעיות חשובות של תורת המספרים. פתרון של משוואות פל הוא בעיה לא קלה, אך פתירה באמצעות כלים אלמנטריים. מטרתנו הסופית היא תיאור מלא של פתרונות המשוואות האלה. תוך כדי נפגוש כמה מושגים ומשפטים שממבט ראשון לאו דווקא נראים קשורים למשוואות פל. לרובם יש חשיבות בפני עצמם, ולא רק ככלים לפתרון של משוואות פל.

בהתחלה נבין איך פותרים משוואות דיאופנטיות לינאריות. פורמלית, לא נשתמש בתוצאות אלה עבור הפתרון של הבעיה העקרית. אבל זה יכול לשמש אותנו כאימון מסויים לפני התמודדות עם החומר היותר מסובך שיבוא בהמשך. החלק החשוב של פתרון משוואות דיאופנטיות לינאריות הוא אלגוריתם אוקלידס שמיועד למציאת מחלק משותף מקסימלי של מספרים שלמים. כאן נגלה, שפעולות חשבון מוגדרות לא רק על

מספרים, אלא גם על אובייקטים מתמטיים אקזוטיים יותר, כגון, למשל, נקודות המישור. בדרך נצטרך גם את למה של מינקובסקי על גוף קמור – עובדה גיאומטרית יפה, שבאופן מפתיע מופיעה בפתרון של הרבה בעיות מתורת המספרים. ולבסוף, נכיר את בסיסים של תורת השברים המשולבים שיעזרו לנו למצוא את פתרונות של משוואות פל.

באופן כזה, תוך כדי התקדמות לעבר המטרה שלנו, נגע בכמה נושאים מתמטיים. לא נתמקד בהם במיוחד, אבל לכמה מהם נוסיף בעיות לפתרון עצמי. רוב הבעיות האלה לא ממש קשורות לנושא העיקרי של הספר, אבל בכמה מקרים משתמשים בתוצאות שלהם בהוכחות בהמשך. בסוף הספר ישנם פתרונות והערות עבור כל הבעיות.

קודם כל, נטען שתי הערות. דבר ראשון, לכל m למשוואה (1) יש לפחות שתי פתרונות: $x=\pm 1,\ y=0$. נקרא לפתרונות אלה *טריוויאליים*. דבר שני, מכיוון שבעת שינוי סימן של x או y החלק השמאלי של משוואה (1) לא ישתנה, אנו יכולים להסתפק במציא של פתרונות אי-שליליים בלבד (המילים אחרות, פתרונות בהם x ו-y אי-שליליים).

במסגרת פתרון של משוואת פל נרצה לענות על שלוש שאלות הבאות:

1) האם קיים פתרון לא טריוויאלי?
2) אם כן, איך למצוא אותו?
3) איך לתאר את קבוצה של כל הפתרונות?

יותר נוח לענות על השאלות האלה בסדר אחר. אנחנו נתחיל דווקא מהשאלה האחרונה: בהנחה שכבר מצאנו פתרון אחד, נראה איך למצוא את כל הפתרונות (ונגלה שיש אינסוף כאלה). אחרי זה נעבור לשאלה ראשונה, ספציפית, נוכיח כי למשוואת פל תמיד יש פתרון לא טריוויאלי. ולבסוף, נראה איך למצוא את הפתרון הזה.

נשים לב, כי הגבלה על הפרמטר m הינה הגבלה טבעית. אם m הוא ריבוע שלם, אז למשוואה (1) אין פתרונות לא טריוויאליים. אכן, הפרש של שני ריבועים (החלק השמאלי של המשוואה) יכול להיות 1, רק אם ראשון מהם שווה לאחד, ושני – לאפס.

דוגמא: משוואה $x^2-2y^2=1$

בהתחלה נפתור משוואת פל עבור $m=2$.

חישוב לא מסובך מראה כי אם זוג (x,y) הינו פתרון של השמוואה לעיל, אז הזוג $(3x+4y,\ 2x+3y)$ גם הוא פתרון. אכן,

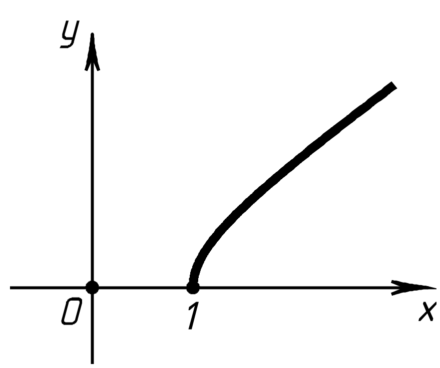
$$(3x+4y)^2-2(2x+3y)^2=$$
$$=(9x^2+24xy+16y^2)-2(4x^2+12xy+9y^2)=x^2-2y^2$$

לכן, אם $x^2-2y^2=1$, אז גם $(3x+4y)^2-2(2x+3y)^2=1$.

זאת אומרת שבהנתן הפתרון הטריוויאלי $x_0=1,\ \mathrm{y}_0=0$ אנחנו יכולים לקבל סדרה אינסופית של פתרונות (לא טריוויאליים) $(x_i,\ \mathrm{y}_i)$ כך שכל אחד מהזוגות מתקבל מהזוג הקודם על ידי נוסחת נסיגה $(x_i,\ \mathrm{y}_i)=f(x_{i-1},\ \mathrm{y}_{i-1})$, כאשר $f(x,y)=(3x+4y,\ 2x+3y)$. הנה כמה איברים ראשונים של הסדרה: $(3,\ 2),\ (17,\ 12),\ (99,\ 70),\ (577,\ 408)$.

נוכיח עכשיו שהסדרה $(x_i,\ \mathrm{y}_i)$ מכסה את כל הפתרונות האי-שליליים. זה יסיים את התיאור של הפתרונות של המשוואה.

את הפתרונות האי-שליליים של משוואת פל אפשר לסדר בצורה טבעית. בשביל זה נתבונן בקבוצת נקודות על מישור קרטזי שמקיימות את הנוסחה $x^2-2y^2=1$ ונמצאות ברביע הראשון של המישור. קבוצה של כל הנקודות האלה הינה גרף של הפונקציה $y=\sqrt{\dfrac{x^2-1}{2}}$ שמוגדרת עבור $x\ge 1$ (ראה איור 1).



איור 1

נגיד שנקודה על הגרף הזה גדולה, אם היא רחוקה מנקודה $(1,\ 0)$. בגלל שהפונקציה אי-שלילית ועולה, משתי נקודות "היותר גדולה" תהיה זאת, שגם

קואורדינטת ה- x, גם קואורדינטת ה- y שלה יהיו יותר גדולות. הפתרונות האי-שליליים של משוואת פל הם בדיוק הנקודות השלמות על הגרף. לכן אי-שוויון $(x', y') < (x'', y'')$ עבור שני פתרונות אי-שליליים שונים (x', y') ו- (x'', y'') אומר כי $x' < x''$ (ששקול ל- $y' < y''$).

ההעתקה f הינה מונוטונית עבור הסדר שהוגדר לעיל. (אנחנו יכולים לדמיין את המונוטוניות גם בצורה הבאה: אם נפעיל את פונקציה f על שתי נקודות, אז תוצאה של הנקודה שנמצאת יותר למעלה ומימינה גם היא תהיה יותר למעלה ומימינה.) אכן, עבור x', y', x'', y'' אי-שליליים מהאי-שוויונות $x' < x''$ ו- $y' < y''$ נובע בברור כי $3x' + 4y' > 3x'' + 4y''$ וגם $2x' + 3y' > 2x'' + 3y''$. כל העתקה מונותונית יש לה העתקה הפוכה שגם היא מונוטונית. ההעתקה ההפוכה ל- f היא $g(x, y) = (3x - 4y,\ 3y - 2x)$. ברור שגם g מעבירה כל פתרון של המשוואה לפתרון.

נניח עכשיו כי קיים פתרון (x', y') למשוואה $x^2 - 2y^2 = 1$ ששונה מכל איבר של סדרה $(x_i,\ y_i)$ שבנינו. בגלל ש- x_i ו- y_i עולים לאינסוף, הפתרון (x', y') נמצא בין שני פתרונות של הסדרה: $(x_i,\ y_i) < (x', y') < (x_{i+1},\ y_{i+1})$. אם נפעיל על אי-שויון זה את ההתעקה המונוטונית g פעם אחרי פעם i פעמים, נקבל $(x_0,\ y_0) < g^i(x', y') < (x_1,\ y_1)$, כאשר $g^i(x', y')$ הוא גם פתרון של המשוואה. אבל לא קשה לוודא כי אין למשוואה פתרונות בין $(1, 0)$ ל- $(3, 2)$. הסתירה שהתקבלה מראה כי כל פתרון אי-שלילי של המשוואה שייך לסדרה $(x_i,\ y_i)$.

באופן דומה אפשר לתאר גם פתרונות של משוואות פל אחרות. בשביל זה מספיק למצוא פונקציה דומה להעתקה f עבור ערך שרירותי של פרמטר m. ההעתקה הזאת אמורה להעביר כל פתרון אי-שלילי של משוואת פל לפתרון אי-שלילי נוסף, והיא חייבת להיות מונוטונית על קבוצת הפתרונות האי-שליליים.

לפני שנתחיל עם פתרון של משוואות פל במקרה הכללי, נבין איך פותרים סוג יותר פשוט של משוואות דיאופנטיות – משוואות דיאופנטיות לינאריות.

משוואות דיאופנטיות לינאריות

משוואה דיאופנטית לינארית היא משוואה דיאופנטית מהצורה

$$ax+by=c \tag{2}$$

כאשר a, b ו- c - מספרים שלמים, ובנוסף a ו- b לא יכולים להיות שווים ל-0 בו-זמנית.

בהתחלה נענה על השאלה, האם יש למשוואה דיאופנטית לינארית לפחות פתרון אחד. נסמן כ- d המחלק המשותף המקסימלי של a ו- b. אם c לא מתחלק ב- d, ברור כי אין פתרונות, כי במקרה הזה החלק השמאלי של ביטוי (2) מתחלק ב- d, והחלק הימיני – לא.

נניח עכשיו ש- $c=kd$. במקרה הזה פתרון קיים. כדי להוכיח את זה, מספיק להראות כי יש פתרון למשוואה

$$ax+by=d \tag{3}$$

אכן, אם נכפיל את הפתרון (כלומר, כל אחד ממספרים x ו- y) ב- k, נקבל את משוואה (2). אחת השיטות למציאת פתרון למשוואה (3) מבוסס על אלגוריתם אוקלידס.

אלגוריתם אוקלידס

אלגוריתם אוקלידס מיועד למציאת מחלק משותף מקסימלי של שני מספרים טבעיים. הוא מבוסס על העובדה הפשוטה הבאה: אם $a=bq+r$ (כאשר q - מנה, ו- r - שארית של חילוק של a ב- b), אז $\gcd(a,\ b)=\gcd(b,\ r)$. אכן, מנוסחא של חילוק עם שארית נובע כי כל מחלק משותף של מספרים b ו- r מחלק גם את a, וגם כל מחלק משותף של a ו- b מחלק גם את r. לכן קבוצות מחלקים משותפים של זוגות מספרים $(a,\ b)$ ו- $(b,\ r)$ שוות, ולכן גם מחלקים משותפים מקסימליים שלהם שווים.

מימוש של אלגוריתם אוקלידס הינו סדרה של פעולות חילוק. בהתחלה מחלקים את המספר היותר גדול במספר היותר קטן. בכל שלב הבא מחלקים את המחלק מהשלב הקודם בשארית של השלב הקודם. ממשיכים באופן כזה עד שמגיעים לשארית שווה ל-0. זה חייב לקרות אחרי מספר סופי של מהלכים, בגלל ששאריות קטֵנות ממש כל הזמן. השארית הלא אפסית האחרונה תהיה המחלק המשותף המקסימלי של שני המספרים המקוריים.

שלבים של אלגוריתם אוקלידס שהפעלנו על זוג $(a,\ b)$ אפשר לרשום בצורה הבאה:

$$\begin{aligned}
a &= bq_1 + r_1 \\
b &= r_1 q_2 + r_2 \\
r_1 &= r_2 q_3 + r_3 \\
&. \ . \ . \ . \ . \ . \ . \ . \\
r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} \\
r_{n-2} &= r_{n-1} q_n + r_{n-1} \\
r_{n-1} &= r_n q_{n+1}
\end{aligned} \tag{4}$$

אזי $d = \gcd(a,\ b) = \gcd(b,\ r_1) = ... = \gcd(r_{n-1},\ r_n) = r_n$.

1.[1] הוכח כי אם m ו-n - שני מספרים שלמים אי-שליליים, אז מספרים $2^{2^m}+1$ ו-$2^{2^n}+1$ הינם זרים.

עכשיו נראה איך למצוא את פתרון של משוואה (3) בהינתן סדרת השוויונות (4). נחלץ $d = r_n$ מהשוויון האחרון. נציב לתוך ביטוי שקיבלנו את r_{n-1} מהשוויון הקודם, וככה הלה. כשנסיים את התהליך, נקבל ביטוי של d כחלק שמאלי של משוואה (3).

בתור דוגמא נתבונן במשוואה $355x + 78y = 1$. בהתחלה נמצא מחלק משותף מקסימלי של מספרים 355 ו-78 בעזרת אלגוריתם אוקלידס:

---

[1] קטעי הטקסט עם שני קווים אנכיים אלה בעיות לפתרון עצמי. הבעיות הקשות ביור מסומנות בכוכבית.

$$355 = 78\cdot 4 + 43$$
$$78 = 43\cdot 1 + 35$$
$$43 = 35\cdot 1 + 8$$
$$35 = 8\cdot 4 + 3$$
$$8 = 3\cdot 2 + 1$$
$$3 = 2\cdot 1 + 1$$
$$2 = 1\cdot 2$$

לכן, $\gcd(355,\ 78) = 1$. נעתיק את השוויונים שקיבלנו בצורה הבאה:

$$43 = 355 - 78\cdot 4$$
$$35 = 78 - 43\cdot 1$$
$$8 = 43 - 35\cdot 1$$
$$3 = 35 - 8\cdot 4$$
$$2 = 8 - 3\cdot 2$$
$$1 = 3 - 2\cdot 1$$

עכשיו נעבור על סדרת השוויונות בסדר הפוך:

$$\begin{aligned}1 &= 3 - 2\cdot 1 = 3 - (2 = 8 - 3\cdot 2)\cdot 1 = 3\cdot 3 - 8 = (35 - 8\cdot 4)\cdot 3 - 8 = \\ &= 35\cdot 3 - 8\cdot 13 = 35\cdot 3 - (43 - 35\cdot 1)\cdot 13 = 35\cdot 16 - 43\cdot 13 = \\ &= (78 - 43\cdot 1)\cdot 16 - 43\cdot 13 = 78\cdot 16 - 43\cdot 29 = 78\cdot 16 - (355 - 78\cdot 4)\cdot 29 = \\ &= 78\cdot 132 - 355\cdot 29\end{aligned}$$

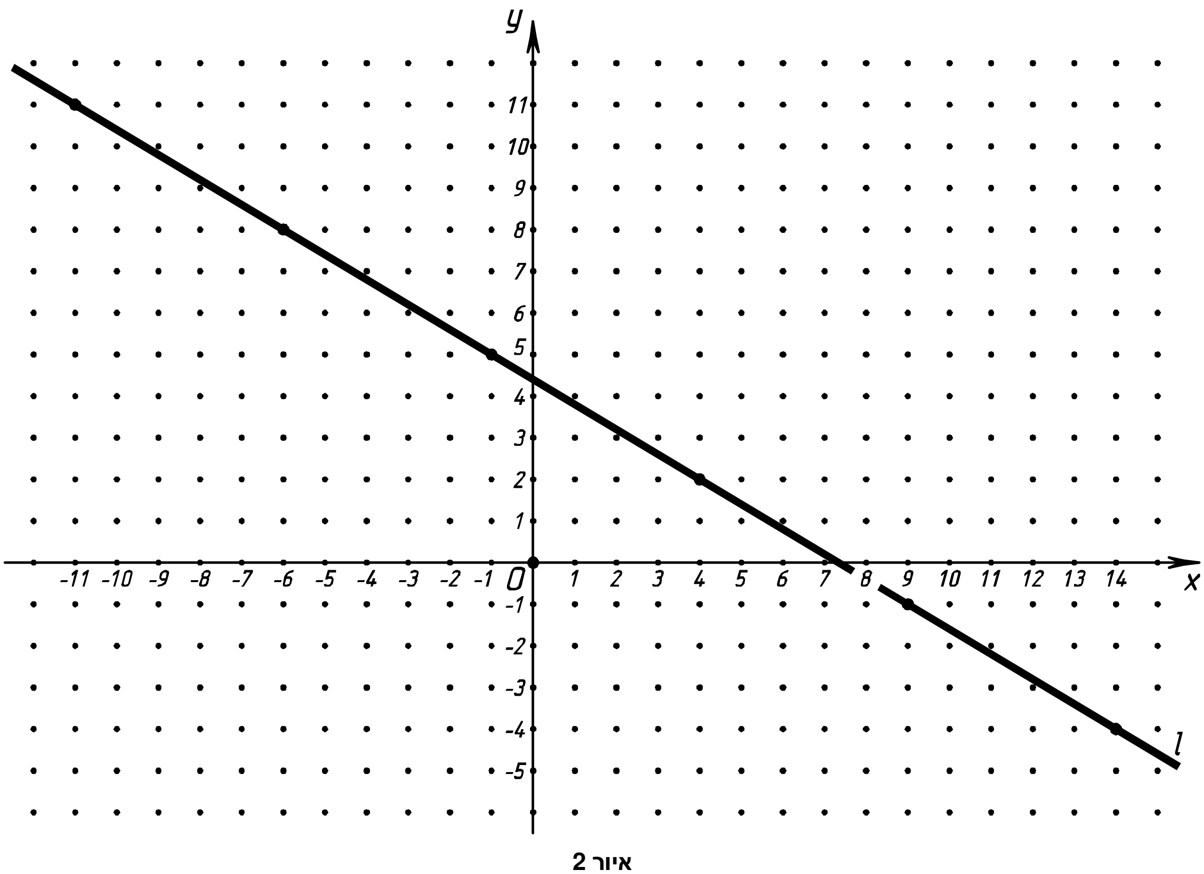
מצאנו פתרון: $x = -29,\ y = 132$.

נשאר לנו לענות על שאלה הבאה: איך בהינתן פתרון אחד של משוואה לינארית נתונה אפשר למצוא את כל הפתרונות שלה? נראה את זה על הדוגמה הבאה.

דוגמא: משוואה $3x+5y=22$

אנחנו יכולים די מהר למצוא אחד פתרונות על ידי לעבור על כל המספרים לפי סדר: $x=4,\ y=2$. (שימוש באלגוריתם אוקלידס יתן פתרון אחר: $x=44,\ y=-23$.)

נצייר במערכת צירים *גרף של המשוואה* – קבוצת נקודות $(x,\ y)$ שמקיימות את המשוואה. הגרף הזה הינו קו ישר (ראה איור 2), נסמן אותו ב-l. על הישר הזה צריך למצוא את כל הנקודות עם קואורדינטות שלמות (לשם פשטות נקרא להם *נקודות שלמות*). מהציור רואים כי נקודות $(4,\ 2)$ ו-$(-1,\ 5)$ שייכות לישר l ואין נקודות שלמות נוספות בקטע שמחבר אותן. כמובן, גרף לא יכול להוות הוכחה לעובדה זאת, אבל ההוכחה עצמה לא הרבה יותר מסובכת. כדי להראות שזה נכון, אפשר פשוט לעבור על כל ה-Y-ים בקטע ולהראות שה-X-ים המתאימים אינם שלמים.



איור 2

נשים לב כי אם זוג (x_0, y_0) הינו פתרון למשוואה, אז זוג (x_0-5, y_0+3) גם פתרון: $3(x_0-5)+5(y_0+3)=3x_0-15+5y_0+15=3x_0+5y_0=22$.

אנחנו רואים שהעתקה

$$(x, y) \mapsto (x-5, y+3) \tag{5}$$

מקיימת שני תנאים הבאים:

א. שומרת על ישר l (ההעתקה מהווה הזזה לאורך הישר הזה)
ב. מעבירה נקודות שלמות לנקודות שלמות

לכן כל פתרון היא מעבירה לפתרון.

אם נפעיל את ההעתקה (5) על פתרון שכבר מצאנו, כלומר, ל- x נוסיף -5, ול- y נוסיף 3 , נקבל פתרון נוסף, וככה הלה. נקודות שמתאימות לכל הפתרונות האלה נמצאות על ישר l במרחקים שווים זו מזו (ראה איור 2). ברור כי אפשר לנוע גם בכיוון ההפוך.

באופן כזה, מצאנו סדרה אינסופית של פתרונות

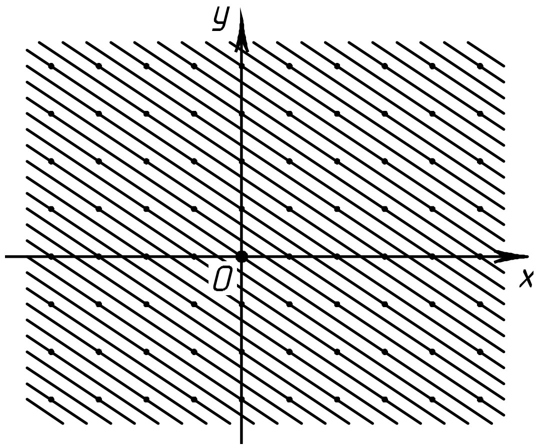
$$x=4-5t,\ y=2+3t$$

כאשר t הוא מספר שלם כלשהו. נוכיח עכשיו שכל הפתרונות של המשוואה הם מהצורה הזאת. נניח בשלילה כי על ישר l בין נקודות $(4-5t, 2+3t)$ ו- $(4-5(t+1), 2+3(t+1))$ יש נקודה שלמה. נפעיל מספר פעמים הזזה (5) במקרה $t>0$, או ההזזה ההפוכה במקרה $t<0$, ונקבל כי בקטע בין נקודות $(4, 2)$ ו- $(-1, 5)$ גם יש נקודה שלמה. סתירה.

בזאת מצאנו את כל הפתרונות של המשוואה והוכחנו כי אין לה פתרונות נוספים.

פתרון כללי של משוואה דיאופנטית לינארית

נעבור עכשיו למקרה כללי. נתבונן בגרפים של משוואות (2) עבור a ו-b קבועים, ו-c פרמטר שעובר על כל המספרים השלמים.
התמונה שנקבל היא משפחה אינסופית של ישרים מקבילים l_c. נשים לב כי כל נקודה שלמה שייכת בדיוק לישר אחד מהמשפחה (ראה איור 3).



איור 3

נגדיר במישור כרטזי "חיבור של נקודות":

$$(x_1,\ y_1)+(x_2,\ y_2)=(x_1+x_2,\ y_1+y_2)$$

הפעולה הזאת מוגדרת גם על תת-קבוצה של נקודות שלמות. לפעולה זאת יש המחשה גיאומטרית טבעית: חיבור של וקטורים עם התחלה בראשית הצירים וסוף בנקודות הנ"ל. בדומה לחיבור רגיל, יש לפעולה הזאת גם הפעולה ההפוכה: חיסור.

נשים לב לתכונה הבאה של החיבור: אם שתי נקודות נמצאות על ישרים l_m ו-l_n, אז סכום שלהן נמצא על ישר l_{m+n}, והפשר – על ישר l_{m-n}. בדיקה של התכונה היא קלה מאוד, לכן נשאיר אותה בתור תרגיל. מהתכונה הזאת נובע כי אם לנקודה שלמה שנמצאת על ישר l_0, נוסיף את כל אחת מהנקודות שמצאות על ישר l_c נקבל את הנקודות השלמות של ישר l_c. במילים אחרות, כדי למצוא את כל הפתרונות של משוואה (2), צריך למצוא פתרון אחד פרטי ואז להוסיף לו את הפתרון הכללי של המשוואה

$$ax+by=0 \qquad (6)$$

נשאר לפתור את המשוואה הזאת. נגדיר שוב $d=\gcd(a,\ b)$. אז נגדיר $a=a'd,\ b=b'd$, ו-$\gcd(a',\ b')=1$. אז משוואה (6) תקבל צורה

$$a'x = -b'y$$

בגלל ש-$a'x$ מתחלק ב-b' וגם a' זר ל-b', x מתחלק ב-b'. מכאן $x = b't$, ואז $y = -a't$.

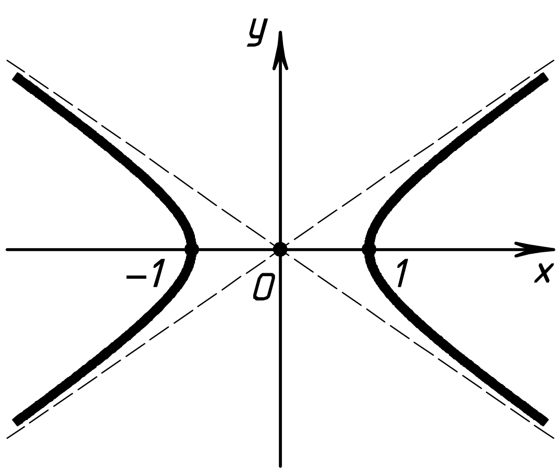
נסכם את כל מה שקיבלנו. אם c לא מתחלק ב-$\gcd(a, b)$, אז למשוואה (2) אין פתרון. אם c כן מתחלק ב-$\gcd(a, b)$, אז למשוואה (2) יש אינסוף פתרונות, וכולם מהצורה:

$$x = x_0 + \frac{b}{d}t,\ y = y_0 - \frac{a}{d}t,$$

כאשר t הוא מספר שלם שרירותי, $d = \gcd(a, b)$, ו- (x_0, y_0) - פתרון פרטי, שאותו אפשר למצוא בעזרת אלגוריתם אוקלידס.

גרף של משוואת פל

דבר ראשון, נצייר גרף של משוואת פל. גרף של המשוואה $x^2 - my^2 = 1$ הינו היפרבולה (ראה איור 4) עם אסימפטוטות $y = \pm\frac{x}{\sqrt{m}}$. כדי לוודא שזה נכון, נפרק את החלק השמאלי של המשוואה לגורמים: $1 = x^2 - my^2 = (x - \sqrt{m}\,y)(x + \sqrt{m}\,y)$, ונכניס מערכת צירים חדשה: נעביר ציר Ox' לאורך הישר $y = -\frac{x}{\sqrt{m}}$, וציר Oy' לאורך הישר $y = \frac{x}{\sqrt{m}}$. במערכת הצרים $Ox'y'$ משוואה של העקום שלנו יראה בצורה "רגילה": $x'y' = const$.



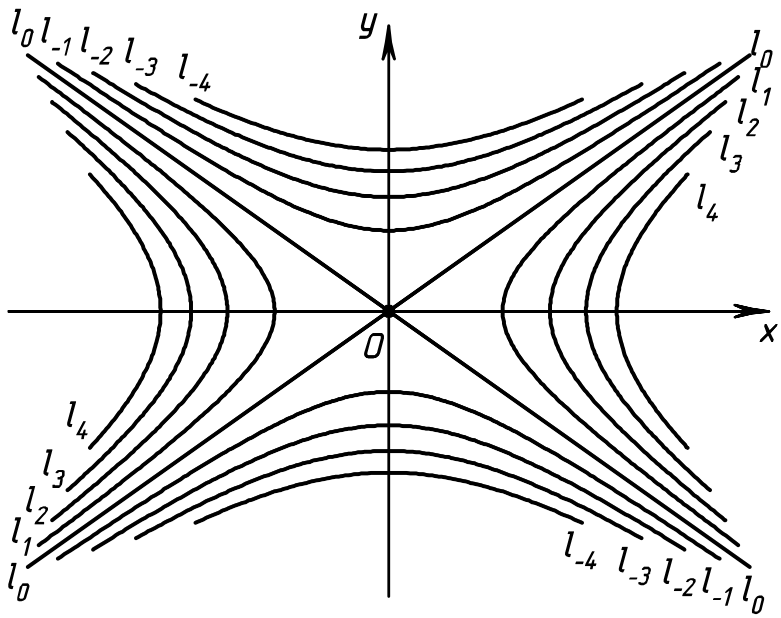
איור 4

לכל m היפרבולה עוברת דרך נקודה $(1, 0)$ וסימטרית יחסית לשני הצירים.

יחד עם ההיפרבולה $x^2 - my^2 = 1$ נתבונן בסדרת העקומים l_n שמוגדרים על ידי המשוואות

$$x^2 - my^2 = n \tag{7}$$

כאשר n עובר על כל המספרים השלמים (ראה איור 5). כאשר $n \neq 0$ העקומים l_n



איור 5

הינם היפרבולות, ו- l_0 זה זוג של הישרים $y = \pm \frac{x}{\sqrt{m}}$ (שמהוות אסימפטוטות משותפות של כל משפחה הזאת של עקומים).

בגלל שלכל נקודה שלמה הגודל $x^2 - my^2$ מהווה מספר שלם, כל נקודה שלמה נופלת על אחד מהישרים l_n. בגלל ש-m אינו ריבוע שלם, על l_0 (זוג האסימפטוטות) יש רק ראשית הצירים, וכל שאר נקודות שלמות נמצאות על ההיפרבולות.

לכל היפרבולה l_n יש היפרבולה *צמודה* l_{-n}. אם נבחר על אחת ההיפרבולות שתי נקודות סימטריות לגבי ראשית הצירים, אז על ההיפרבולה הצמודה לה אפשר לבחור זוג נוסף של נקודות סימטריות לגבי ראשית הצירים, כך שארבעת הנקודדות האלה

יהוו קודקודים של מקבילית עם צדדים מקבילים לאסימפטוטות. לשתי זוגות כאלה של נקודות נקרה *צמודים* זה לזה. אכן, אם במערכת צירים המוגדרת על ידי שתי האסימפטוטות לזוג של נקודות סימטריות יש קואורדינטות (x', y') ו-$(-x', -y')$, אז זוג הנקודות הצמוד לה במערכת צירים הזאת הוא זוג הבא של נקודות סימטריות: $(x', -y')$ ו-$(-x', y')$.

כפל נקודות

כשדיברנו על משוואות דיאופנטיות לינאריות, הגדרנו "חיבור" של נקודות המישור, והפעולה הזאת עזרה לנו להבין איך בנויים הפתרונות של המשוואות האלה.

עכשיו אנחנו נגדיר פעולה נוספת על נקודות המישור. נקרא לפעולה הזאת "כפל", והיא תעזור לנו לפתור את משוואת פל. יותר מדוייק, אנחנו נגדיר לא פעולה אחת, אלא משפחה אינסופית של פעולות (שתלויות בפרמטר m שיש עליו מגבלה שאינו ריבוע שלם – כמו במשוואות פל). הנה הגדרה של כפל נקודות:

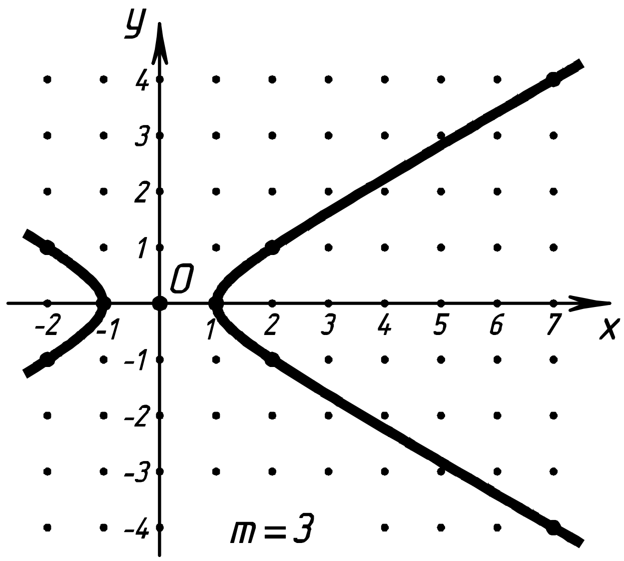
$$(x_1,\ y_1)\cdot(x_2,\ y_2) = (x_1x_2 + my_1y_2,\ x_1y_2 + x_2y_1) \tag{8}$$

הפעולה שהגדרנו מקיימת אותם תנאיים כמו הכפל הרגיל: קומוטטיביות, אסוציאטיביות ודיסטריבוטיביות ביחס לחיבור נקודות שהגדרנו קודם. את התכונות האלה אפשר לבדוק בדרך ישירה, אך לא נמהר להתחיל לרשום שורות ארוכות של חישובים. הוכחות ללא שום חישובים יבואו בהמשך, אחרי שנבין את הפרשנות האלגברית של הכפל שלנו.

אם נקודה $(x_1,\ y_1)$ שייכת לעקום l_n, ונקודה (x_2, y_2) שייכת לעקום l_k, אז מכפלתן $(x_1,\ y_1)\cdot(x_2,\ y_2)$ שייכת לעקום l_{n+k}. אכן,

$$\begin{aligned}
&(x_1x_2 + my_1y_2)^2 - m(x_1y_2 + y_2x_1)^2 = \\
&= {x_1}^2{x_2}^2 + 2mx_1x_2y_1y_2 + m^2{y_1}^2{y_2}^2 - m{x_1}^2{y_2}^2 - 2mx_1x_2y_1y_2 - m{y_1}^2{x_2}^2 = \\
&= ({x_1}^2 - m{y_1}^2)({x_2}^2 - m{y_2}^2) = n\cdot k
\end{aligned}$$

בפרט, אם נכפיל נקודות שנמצאות על l_1, נקבל נקודות שנמצאות על l_1. במילים אחרות, מכפלה של פתרונות של משוואת פל הינה גם פתרון. כפל בפתרון האי-שלילי הטריוויאלי לא יתן לנו פתרונות נוספים, כי הנקודה $(1,\ 0)$ משחקת פה תפקיד של "אחד": אם נכפיל בה נקודה מסויימת, נקבל אותה נקודה בחזרה.



איור 6

פתרון כללי של משוואת פל

אם למשוואת פל יש לפחות פתרון לא טריוויאלי אחד, אז אם נכפיל אותו אינסוף פעמים בעצמו, נקבל אינסוף פתרונות.
יחד עם זאת, את כל הפתרונות אפשר למצוא בצורה דומה לאיך שעשינו את זה במקרה של $m = 2$. תוך כדי תנועה מנקודה $(1,\ 0)$ ימינה על פני גרף של משוואה (ראה איור 6), אנחנו מוצאים את הפתרון (הלא טריוויאלי) הראשון. נקרה לפתרון זה *בסיסי*.

משפט 1. כל פתרונות לא טריוויאליים של משוואת פל מתקבלים מכפל (מספר פעמים) של הפתרון הבסיסי בעצמו.

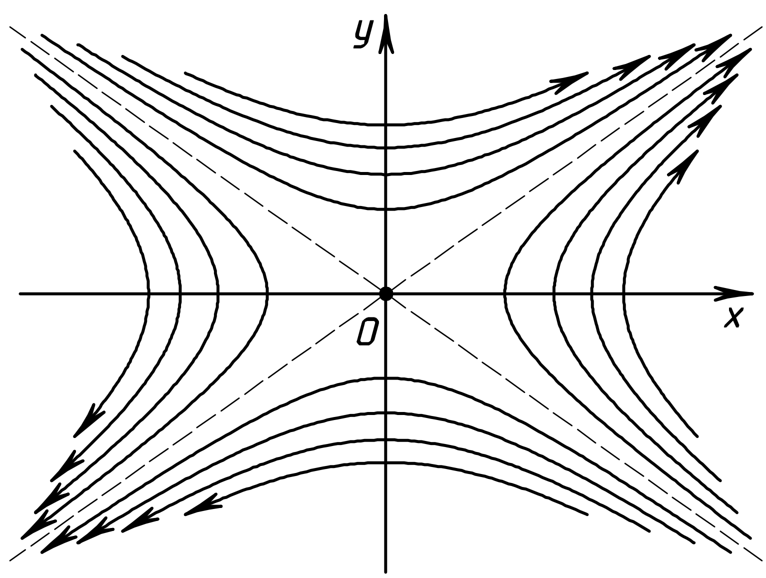
הוכחה. נתבונן בסדרה $(x_1,\ y_1),\ (x_2,\ y_2),\ \ldots\ (x_n,\ y_n),\ \ldots$ של פתרונות שמתקבלים מהפתרון הבסיסי $(x_1,\ y_1)$ על ידי כפל בעצמו. נניח שבגרף המשוואה קיים פתרון נוסף שנמצא בין שני איבריה: $(x_n,\ y_n)$ ו-$(x_{n+1},\ y_{n+1})$. אם נכפיל אותו ב- $(x_1,\ -y_1)$, נקבל פתרון חדש של המשוואה שנמצא בין $(x_{n-1},\ y_{n-1})$ ל-$(x_n,\ y_n)$. אכן, כפל ב-$(x_1,\ -y_1)$ הינו פעולה הפוכה לכפל ב-$(x_1,\ y_1)$. אם נחזור על הפעולה n פעמים, נקבל פתרון שנמצא בין $(1,\ 0)$ ל-$(x_1,\ y_1)$. זה סותר את זה ש-$(x_1,\ y_1)$ הינה הפתרון הבסיסי. ■

עכשיו נעבור להוכחת קיום של פתרון לא טרוויאלי למשוואת פל כלשהי. בשביל זה נצטרך להגדיר חילוק של נקודות – פעולה הפוכה לכפל. אבל לפני נראה שתי פרשנויות של כפל נקודות: גיאומטרית ואלגברית.

סיבוב היפרבולי

יהי $(x_0,\ y_0)$ – פתרון לא טריוואלי מסויים של משוואת פל. נתבונן בהעתקה שמעביר כל נקודה שרירות $(x,\ y)$ לנקודה $(x_0x+my_0y,\ x_0y+y_0x)$. ההעתקה הזאת – כפל בפתרון לא טריוויאלי של משוואת פל – מעבירה כל נקודה על היפרבולה l_n לנקודה נוספת עליה, כלומר את כל היפרבולה מהמשפחה היא מזיזה לאורך עצמה (ולכן היא נקראת *סיבוב היפרבולי*). תוך כדי הפעולה נקודות שלמות עוברות לנקודות שלמות.

כיוונים בהם מוזזות ההיפרבולות מצויינים באיור 7 (מנחים שהפתרון הבסיסי $(x_0,\ y_0)$ חיובי).



איור 7

כשדיברנו על משוואות דיאופנטיות לינאריות, תפקיד תואם היה להזזות לוקטורים שלמים לאורך גרף של משוואה (ישר).

2. שאלה לבדיקת הבנה. איך ההעתקה הנ"ל משפיעה על האסימפטוטות?

עכשיו ברצנינו להציע סדרה של משוואות דיאופנטיות מסדר שני שקרובות למשוואות פל לפתרון עצמי.

3. הוכח כי מספרים שלמים אי-שליליים x, y מקיימים את המשוואה $x^2 - mxy + y^2 = 1$ (כאשר m הוא פרמטר שלם נתון) אם ורק אם x ו-y הינם איברים עוקבים של הסדרה

$$\varphi_0 = 0,\ \varphi_1 = 1,\ \varphi_2 = m,\ \varphi_3 = m^2 - 1,\ \varphi_4 = m^3 - 2m,$$
$$\varphi_5 = m^4 - 3m^2 + 1,\ \ldots\ \varphi_{k+1} = m\varphi_k - \varphi_{k-1}$$

מספרים אי-רציונליים מדרגה שנייה

נתבונן בקבוצה $\mathbb{Z}[\sqrt{m}]$ של מספרים מהצורה $x + \sqrt{m}y$, כאשר x ו-y שלמים. לא קשה להבין כי סכום, הפרש ומכפלה של איברי $\mathbb{Z}[\sqrt{m}]$ שייכים ל-$\mathbb{Z}[\sqrt{m}]$ גם הם:

$$(x_1 + \sqrt{m}y_1) \pm (x_2 + \sqrt{m}y_2) = (x_1 \pm x_2) + (y_1 \pm y_2)\sqrt{m}$$

$$(x_1 + \sqrt{m}y_1) \cdot (x_2 + \sqrt{m}y_2) = (x_1x_2 + my_1y_2) + (x_1y_2 + x_2y_1)\sqrt{m}$$

אנחנו רואים שאם נתאים לכל מספר מהצורה $x + \sqrt{m}y$ נקודה (x, y) במישור, נראה שפעולות חיבור וכפל על המספרים תתאים לחיבור וכפל על נקודות שהגדרנו. בגלל שכפל של המספרים הוא קומוטטיבי, אסוציאטיבי ודיסטריבוטיבי, תחונות אלה מתקיימות גם עבור נקודות המישור.

נשים לב כי ההתאמה הזאת בין $\mathbb{Z}[\sqrt{m}]$ ונקודות שלמות של המישור היא חד-חד-ערכית ועל: הנחה שלשתי נקודות שונות $(x_1,\, y_1)$ ו- $(x_2,\, y_2)$ מתאים אותו מספר גוררת שוויון $x_2 + y_2\sqrt{m} = x_1 + y_1\sqrt{m}$, ומכאן $\sqrt{m} = \dfrac{x_1 - x_2}{y_1 - y_2}$. זה לא יתכן כי $\sqrt{m}$ אי-רציונלי.

לכל מספר $x + y\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ אפשר להגדיר את *המספר הצמוד* $\overline{x + y\sqrt{m}} = x - y\sqrt{m}$ *ונורמה* $N(x + y\sqrt{m}) = x^2 - my^2$, שהיא שווה גם למכפלה של המספר בצמוד. נשים לב שנורמה של מספר שווה למספר היפרבולה עליה נופלת נקודה המתאימה למספר.

את העובדה שמכפלה של שתי נקודות נמצאת על היפרבולה עם מספר ששווה למכפלה של מספרים של היפרבולות של הנקודות הנ"ל אפשר לנסח מחדש בצורה הבאה: נורמה של מכפלה שווה למכפלת הנורמות.

במונחים אלה לפתור משוואת פל זה אותו דבר כמו למצוא את כל מספרים ב- $\mathbb{Z}[\sqrt{m}]$ עם נורמה שווה לאחד.

תוצאת חילוק של שני מספרים $x_1 + y_1\sqrt{m}$ ו- $x_2 + y_2\sqrt{m}$ מ- $\mathbb{Z}[\sqrt{m}]$ לאו דווקה שייכת ל- $\mathbb{Z}[\sqrt{m}]$. זה קורה רק במקרה ש- $x_1x_2 - my_1y_2$ ו- $x_2y_1 - x_1y_2$ מתחלקים ב- $N(x_2 + \sqrt{m}\,y_2)$. אכן,

$$\frac{x_1 + y_1\sqrt{m}}{x_2 + y_2\sqrt{m}} = \frac{(x_1 + y_1\sqrt{m})(x_2 - y_2\sqrt{m})}{(x_2 + y_2\sqrt{m})(x_2 - y_2\sqrt{m})} =$$

$$= \frac{x_1x_2 - my_1y_2}{N(x_2 + y_2\sqrt{m})} + \frac{x_2y_1 - x_1y_2}{N(x_2 + y_2\sqrt{m})}\sqrt{m}$$

בפרט, כשנורמה של מספר שווה ל- ± 1, אז כל המספרים מתחלקים בו. נצטרך את הטענה הבאה:

למה 1. יהיו $x_1 + y_1\sqrt{m}$ ו- $x_2 + y_2\sqrt{m}$ שייכים ל- $\mathbb{Z}[\sqrt{m}]$, $n = \left|N(x_2 + y_2\sqrt{m})\right|$. אם $x_1 \equiv x_2 (\bmod n)$ וגם $y_1 \equiv y_2 (\bmod n)$, אז $x_1 + y_1\sqrt{m}$ מתחלק ב- $x_2 + y_2\sqrt{m}$.

הוכחה. לפני הגדרת הנורמה, $\left|x_2^2 - my_2^2\right| = n$, לכן $x_2^2 - my_2^2 \equiv 0 (\bmod n)$. נתון ש- $x_1 \equiv x_2 (\bmod n)$, לכן $x_1 x_2 \equiv x_2^2 (\bmod n)$. באופן דומה, מ- $y_1 \equiv y_2 (\bmod n)$ נובע $my_1 y_2 \equiv my_2^2 (\bmod n)$. נחסיר ונקבל:

$$x_1 x_2 - my_1 y_2 \equiv x_2^2 - my_2^2 \equiv 0 (\bmod n) \tag{9}$$

חוץ מזה, אם נקח את שתי הקונגרואנציות מהנתון ונכפיל אותן (אחת כמושהי והשנייה בסדר הפוך), נקבל $x_2 y_1 \equiv x_1 y_2 (\bmod n)$, או, במילים אחרות

$$x_2 y_1 - x_1 y_2 \equiv 0 (\bmod n) \tag{10}$$

קונגרואנציות (9) ו-(10) מראות כי $x_1 + y_1\sqrt{m}$ מתחלק ב- $x_2 + y_2\sqrt{m}$. ■

חילוק נקודות

נחזור לנקודות השלמות הממוקמות על משפחת ההיפרבולות. כל מה שנאמר על התחלקות של מספרים ב- $\mathbb{Z}[\sqrt{m}]$, תקף גם עבור התחלקות של נקודות, כתוצאה מיחס חח"ע ועל שגילינו בפרק הקודם. נראה כי קיימת היפרבולה l_n שיש עליה שתי נקודות שמתחלקות אחת בשנייה. בשביל זה מספיק להראות כי על ההיפרבולה יש לפחות $n^2 + 1$ נקודות שלמות. אכן, קיימות רק n^2 אפשרויות לזוג שאריות שקואורדינטות של נקודה יכולות לתת בחילות ב- n. לכן, לפי עקרון שובך יונים, בכל קבוצה שמכילה $n^2 + 1$ נקודות שלמות, לשתיים מהנקודות האלה גם קואורדינטת ה- x, גם קואורדינטת ה- y שוות מודולו n. לפי למה 1, הנקודות האלה מתחלקות אחת

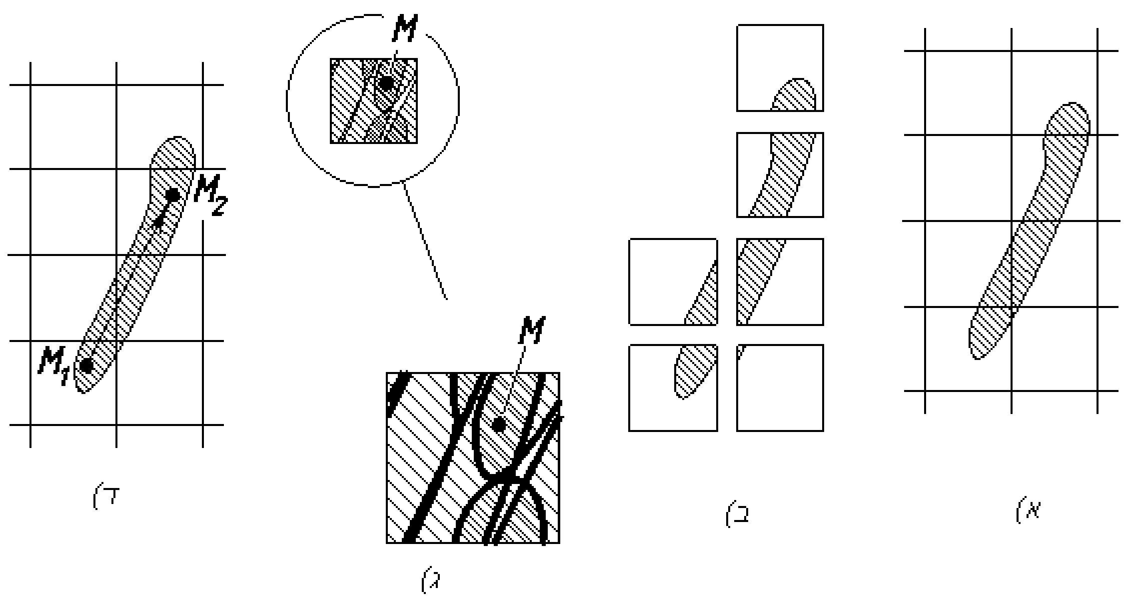
בשנייה. תוצאת החילוק חייבת להיות שייכת להיפרבולה l_1, במילים אחרות, להיות פתרון של משוואת פל. בגלל שהנקודות שנבחרו שונות ואי-שליליות, הפתרון הזה לא טריוויאלי.

נעזוב לרגע את החלק האלגברי ונדבר על כמה עובדות גיאומטריות יפות. אחרי זה נוכיח שעל אחת ההיפרבולות יש אינסוף נקודות שלמות. זה יסיים את הוכחה של קיום פתרון למשוואת פל.

למה של מינקובסקי על גוף קמור

אנחנו הולכים להוכיח שתי למות גיאומטריות מגניבות. הלמה הראשונה משחקת תפקיד של שלב ביניים בהוכחת הלמה השנייה. הלמה השנייה נקראת למת מינקובסקי, והיא בצורה מפתיעה תהווה החלק העקרי בהוכחת קיום של פתרון של משוואת פל.

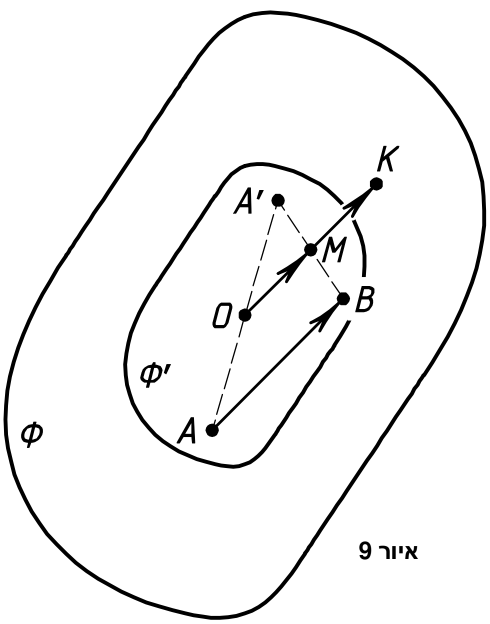
למה 2. תהי Φ צורה במישור עם שטח גדול מ-1. אזי קיימות שתי נקודות A ו-B השייכות ל-Φ כך שווקטור $\overrightarrow{AB}$ (במילים אחרות, אפשר להזיז את הצורה Φ לאורך וקטור שלם כך שהיא תחתוך את העותק של עצמה).



איור 8

הוכחה. נחתוך את המישור הקרטזי לריבועים עם צלע 1 על ידי ישרים מקבילים לצירים (איור 8, א, ב). את כל הריבועים שיש להם לפחות נקודת חיתוך אחת עם Φ, נזיז כך שהם כולם יתלכדו. בשביל זה אחד מהריבועים נשאיר במקום, ושאר נזיז לאורך וקטורים שלמים כך שהם יכלכדו עם הריבוע הראשון. אחרי זה כל החתיכות של צורה Φ נמצאות בתוך ריבוע אחד. בגלל ששטח של Φ גדול מ-1, חתיכות מסויימות נחתכות. תהי M נקודה משותפת איזושהי של שתי חתיכות שונות (ראה איור 8, ג). נעביר את כל החתיכות למקומות שלהן (על ידי ההזזות ההפוכות). נקודה M תעבור לנקודות בתוף Φ שמהוות קצוות של וקטור שלם (ראה איור 8, ד). ■

למת מינקובסקי. תהי Φ - צורה במישור קרטזי, קמורה, בעלת סימטריה מרכזית (יחסית לראשית הצירים), עם שטח גדול מ-4. אזי היא מכילה נקודה שלמה בנוסף לראשית הצירים.



איור 9

הוכחה. נתבונן בהומותטיה עם מקדם $\frac{1}{2}$ ומרכז בראשית הצירים O. היא מעבירה את צורה Φ לצורה Φ' שגם קמורה וסימטרית יחסית ל-O עם שטח גדול מ-1 (ראה איור 9). מלמה 2, אפשר למצוא נקודות $A,\ B \in \Phi'$ כך שוקטור $\overrightarrow{AB}$ שלם. תהי A' נקודה סימטרית ל-A יחסית ל-O. מסימטריה של הצורה יחסית לראשית הצירים נובע כי $A' \in \Phi'$. עכשיו, תהי M אמצע של קטע $A'B$. מהקמירות נובע כי $M \in \Phi'$. מצד שני,

$$\overrightarrow{OM} = \frac{1}{2}(\overrightarrow{OA'} + \overrightarrow{OB}) = \frac{1}{2}(\overrightarrow{AO} + \overrightarrow{OB}) = \frac{1}{2}\overrightarrow{AB}$$

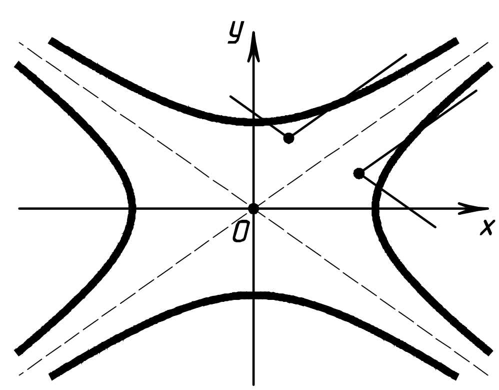
נתבונן בנקודה K כך ש- $\overrightarrow{OK} = 2\overrightarrow{OM}$. בגלל ש- $\overrightarrow{OK} = \overrightarrow{AB}$ - וקטור שלם, K היא נקודה שלמה, ובגלל ש-$M \in \Phi'$, אז גם $K \in \Phi'$. לכן K היא הנקודה שחיפשנו.

4. יש גן בצורת עיגול עם רדיוס של קילומטר אחד. בגן יש עצים שמושתלים בקודקודים של רשת ריבועית עם צלע של מטר אחד (כולל הקודקודים שנמצאים על הקצה של הגן). אם מרחק מקודקוד של הרשת עד קצה של הגן קטן מרדיוס של עץ מסויים, אז העץ חורג מגבולות הגן. הקודקוד היחיד של הרשת בו אין עץ זה מרכז של הגן. רדיוס של כל עץ שווה למילימטר אחד. הוכח שתצפית ממרכז הגן חסומה לגמרי, כלומר, כל קרן שיוצאת משם חותך גזע איזשהו.

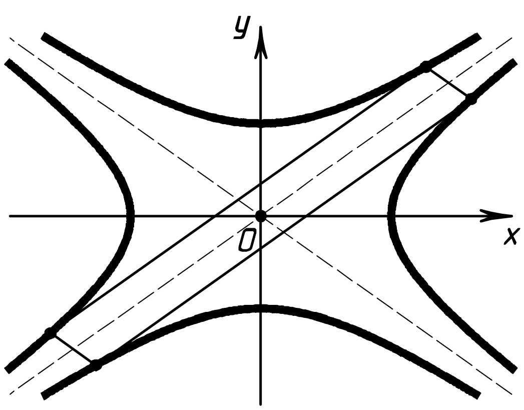
*5. יהיו $a,\ b,\ c$ – מספרים שלמים, ונתון בנוסף כי $a>0,\ ac-b^2=1$. הוכח כי למשוואה $ax^2+2bxy+cy^2=1$ יש פתרון שלם.

סיום של הוכחת קיום של פתרון לא טריוויאלי למשוואת פל

מה שנותר לנו להוכיח זה שעל אחת ההיפרבולות מהמשפחה יש אינסוף נקודות שלמות. נניח בשלילה כי כל היפרבולה מכילה רק מספר סופי של נקודות כאלה. נקח



איור 10

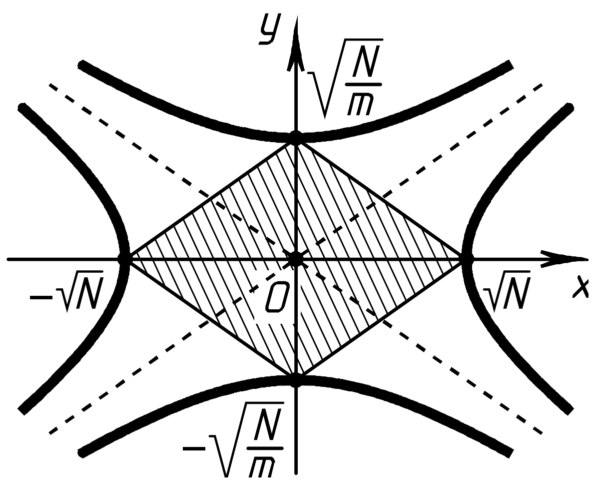


איור 11

היפרבולה l_N עם מספר מספיק גדול (למה צריך להיות שווה N, נגלה בהמשך) וההיפרבולה l_{-N} הצמודה לה. בתוך התחום החסום על ידי שתי ההיפרבולות האלה יש רק מספר סופי של נקודות שלמות. אכן, כל הנקודות האלה שייכות למספר סופי של היפרבולות עם אינדקסים בין $-N$ ל- N, ולפי הנחה, על כל אחת מהן יש רק מספר סופי של נקודות שלמות (כאן באה בחשבון גם ההיפרבולה המנובנת l_0, ועליה יש רק

נקודה שלמה אחת שהיא ראשית הצרים). אסימפטוטות של ההיפרבולות מחלקות את המישור לארבע זוויות, וכל אחת מהנקודות, חוץ מראשית הצירים, נמצאת בתוך אחת מהזוויות הנ"ל. מכל אחת מהנקודות נעביר זוג קרניים המקבילים (וגם באותו כיוון) של צלעות של הזווית המתאימה (ראה איור 10).

נקבל מספר סופי של זוויות כאלה. לכל אחת מהזוויות צלעותיה חותכות את אחד מארבעת הענפים של זוג ההיפרבולות. מכאן, כל זווית מכסה על ההיפרבולות קבוצה חסומה של נקודות. נבחר זוג של נקודות סימטריות על אחת ההיפרבולות והזוג הצמוד לה על ההיפרבולה הצמודה (ראה עמוד 14), באופן כזה שאף אחת מהנקודות האלה לא תכוסה על ידי שום זווית שציירנו.זה אכן אפשרי – מספיק רק לבחור נקודות מספיק רחורות, כי הזוויות מכסות רק תחום חסום על כל אחד הענפים. מקבילית עם קודקודים בנקודות האלה (ראה אייור 11) לא מכילה נקודות שלמות חוץ מראשית הצירים, אחרת זווית שציירנו מהנקודה הזאת הייתה חותכת את אחד הקודקודים של המקבילית. אבל אז אנחנו מקבלים סתירה עם למת מינקובסקי, כי מקבילית היא צורה קמורה עם סימטריה מרכזית, ואם נבחר N מספיק גדול, נוכל לקבל מקבילית עם שטח גדול מ-4.



איור 12

נשאר להראות מה צריך להיות N בשביל זה. נשים לב, כי שטח המקבילית תלוי רק ב- N שהוא מספר ההיפרבולה, ולא בבחירה של נקודות עליה. אכן, שטח של מקבילים פרופורציונלי למכפלה של צלעותיה (מקדם הפרופורציה שווה לסינוס של זווית ביניהם ותלוי רק ב- m). אבל במערכת צירים שצירים שלה מקבילים לאסימפטוטות, צלעות המקבילית שוות פעמיים קואורדינטת- x ופעמיים קואורדינטת- y של אחד הקודקודיו. וההיפרבולה (באותה מערכת הצירים) מוגדרת על ידי המשוואה הבאה: מכפלה של קואורדינטת- x וקואורדינטת- y שווה לקבוע. לכן, בבחירה שרירותית של הקודקודים על ההיפרבולות, שטחה של המקבילית גם יהיה קבוע.

נחזור למערכת הצירים ההתחלתית. מטרתנו לחשב את שטחה של המקבילית. לשם נוחות כדאי לבחור את המקבילית שקודקודיה הינם נקודות חיתוך של ההיפרבולות עם הצירים (ראה איור 12). אלה נקודות $(\pm\sqrt{N},\ 0)$ ו-$(0,\pm\sqrt{\frac{N}{m}})$. המקבילית הזאת הינה מעויין, וקל למצוא את שטחה: $S=\frac{2N}{\sqrt{m}}$. מהנתון $S>4$ מקבלים $N>2\sqrt{m}$.

בזאת, סיימנו את ההוכחה של קיום הפתרון.

משפט 2. לכל משוואת פל קיים פתרון לא טריוויאלי.

הערה. משפט של קיום הפתרון למשוואת פל מהווה מקרה פרטי של משפט דיריכלא על מבנה של חבורת היחידות בחוג המספרים האלגבריים השלמים. המשפט הזה (שלא רק הוכחה, אלא אף ניסוח שלו אינם אלמנטריים) הינו אחת מהתוצאות היפות של תורת המספרים. ניסוח והוכחה של משפט דיריכלא, שהינו בפועל הכללה של זה שיש פה, אפשר למצוא בספר [2].

6. שאלה לבדיקת הבנה. איפה בהוכחה של משפט 2 השתמשנו בזה ש-m אינו ריבוע שלם?

איך למצוא פתרון למשוואת פל

להוכחת קיום פתרון של משוואת פל שהביאנו לעיל יש חסרון משמעותי: זאת הוכחה לא קונסטרוקטיבית. במילים אחרות, ההוכחה לא נותנת שום דרך למציאת פתרון. נשאלת השאלה, איך למצוא פתרון פרטי (רצוי הפתרון הבסיסי) של משוואת פל? יש דרך אחת שהיא "ראש בקיר": לעבור על כל ערכים שלמים אי-שליליים של y עד שמספר my^2+1 יהיה ריבוע שלם. האלגוריתם הזה בטוח יביא אותנו לפתרון הבסיסי מתישהו. אבל אין לנו שום הערכה כמה זמן הוא יעבוד. ואכן, האלגוריתם אינו יעיל

במיוחד. יש ערכים של m די קטנים שעבורם ערכי x ו- y (שמייצגים הפתרון הבסיסי) גדולים. למשל, עבור $m=109$ הכיתוב העשרוני של מספר x מורכב מ-15 ספרות, ושל מספר y מ-14 ספרות. לכן שימוש באלגוריתם הזה אינו מעשי אפילו אם נשתמש במחשב.

בפתרון של משוואות דיאופנטיות לינאריות נעזרנו באלגוריתם אוקלידס שנתן לנו דרך יעילה לפתרון. באופן דומה, בשביל פתרון של משוואות פל נעזר בשברים משולבים.

שברים משולבים

כל מספר α שאינו שלם ניתן להציג בצורה $\alpha=\alpha_0+\frac{1}{\alpha_1}$, כאשר α_0 מספר שלם, ו- $\alpha_1>1$. אכן, בתור α_0 צריך לקחת את החלק השלם של מספר α, ובתור α_1 המספר ההופכי לחלק שברי של α. היצוג הנ"ל הינו יחיד, כי מהתנאי $\alpha_1>1$ נובע $1<\frac{1}{\alpha_1}<0$, לכן $\frac{1}{\alpha_0}$ הינו החלק השברי של α, ולכן α_0 - החלק השלם של α. אם מספר α_1 יצא לא שלם, אז גם אותו אפשר להציג בצורה $\alpha_1=a_1+\frac{1}{\alpha_2}$, וככה הלה.

בסוף נקבל יצוג הבא של מספר α:

$$\alpha=\alpha_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\ddots+\cfrac{1}{\alpha_n}}} \qquad (11)$$

כאן a_0 מספר שלם, $a_1, a_2, \dots a_{n-1}$ – מספרים טבעיים, ו-α_n מספר גדול מ-1, לאו דווקא שלם. עבור n קבוע מראש, הייצוג הזה יחיד. יכול לקרות מצב שעבור n מסויים מספר α_n יוצא שלם, והתהליך יסתיים. במקרה זה החלק הימין של הביטוי (11) נקרא *שבר משולב סופי*. אם אף אחד מ-α_i אינו שלם, אז נקבל הביטוי הבא:

$$\alpha = \alpha_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}} \qquad (12)$$

החלק הימני של הביטוי הזה נקרא *שבר משולב אינסופי*. המקדמים ... $\alpha_0, a_1, a_2,$ נקראים *איברים* של השבר המשולב.

7. שבר משולב הינו סופי אם ורק אם מספר α הינו רציונלי.

אם נאפשר לאיבר אחרון של שבר משולב להיות שווה ל-1, אז יצוג של מספרים רציונליים בתור שבר משולב יפסיק להיות יחיד. לביטויים כאלה נקרא *שברים משולבים סופיים מוכללים*. כל מספר רציונלי אפשר לייצג בצורה של שבר משולב סופי מוכלל בדיוק בשתי דרכים, ומתקיים כי מספר קומות בשני היצוגים האלה שונים ב-1. הדרך הראשונה היא יצוג של המספר בצורה של שבר משולב, והדרך השנייה מתקבלת מהראשונה על ידי החלפת איבר אחרון a_n ב-$(a_n - 1) + \frac{1}{1}$.

8. אם סדרת האיברים של שבר משולב הינה מחזורית, אז מספר α הינו שורש של משוואה ריבועית עם מקדמים שלמים.

הערה. גם הטענה ההפוכה נכונה: אם α שורש אי-רציונלי של משוואה ריבועית במקדמים שלמים, אז סדרת האיברים של השבר המשולב שמייצג את α הינה מחזורית. אבל הוכחה של הטענה הזאת משמעותית יותר מסובכת.

כדי שלביטוי (12) תהיה משמעות, צריך להגדיר בצורה יותר ברורה את החלק הימיני שלו. בשביל זה "נקטע את הזנב" של השבר המשולב האינסופי ונקבל שבר משולב סופי מוכלל:

$$r_n = \alpha_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{\alpha_n}}}$$

השבר הזה מיצג איזשהו מספר רציונלי: $r_n = \frac{p_n}{q_n}$ (את p_n ו- q_n נגדיר בצורה כזאת, שהשבר $\frac{p_n}{q_n}$ הינו מצומצם). נקרא לשבר הזה *השבר המתקרב ה- n-י* של השבר המשולב (וגם של מספר α שהשבר הזה מייצג). שבר מתקרב מוגדר עבור כל $n \geq 0$. נוכיח כי סדרת השברים המתקרבים מתכנסת. אז נוכל באופן טבעי להגדיר את החלק הימיני של ביטוי (12) כגבול של סדרת השברים המתקרבים. בשביל הוכחת קיום הגבול ננסח כמה טענות עזר. שתי הטענות הראשונות נביא כבעיות לפתרון עצמי. שתיהן נפתרות בקלות באינדוקציה.

9. הוכח כי סדרות p_n ו- q_n מקיימות את כללי נסיגה הבאים:

$$\begin{cases} p_{n+1} = p_n a_{n+1} + p_{n-1} \\ q_{n+1} = q_n a_{n+1} + q_{n-1} \end{cases} \qquad (14)$$

נשים לב שכתוצאה מכך הסדרות p_n ו- q_n עולות מונוטונית בערך מוחלט (עבור $n \geq 1$), ושואפות לאינסוף.

10. הוכח כי לכל $n \geq 1$:

$$. p_{n-1}q_n - p_nq_{n-1} = (-1)^n \tag{15}$$

למה 3. אם n זוגי ו-$m > n$, אז $r^n < \alpha$ וגם $r_n < r_m$. אם n אי זוגי ו-$m > n$, אז $r^n > \alpha$ וגם $r_n > r_m$.

הוכחה. נתבונן בפונקציה הבאה במשתנה x:

$$f_n(x) = \alpha_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{x}}} \tag{16}$$

הפונקציה הינה מונוטונית עולה עבור n-ים זוגיים ומונוטונית יורדת עבור n-ים אי-זוגיים. אכן, אפשר להציג אותה כהרכבה של שתי פונקציות n פעמים: פונקציה אחת היא לקחת הופכי, והפונקציה השנייה היא להוסיף קבוע. תוך כדי התהליך, לקיחת הופכי כל פעם הופכת את המונוטוניות להפוכה, והוספת קבוע שומרת עליה.

נסמן:

$$a_{m,n} = \alpha_n + \cfrac{1}{a_{n+1} + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_m}}}$$

אזי $a_n < \alpha_n$, $a_n < a_{m,n}$ ו-$f_n(a_{n,m}) = r_m$, $f_n(\alpha_n) = \alpha$, $f_n(a_n) = r_n$. ממונוטוניות של פונקציה $f_n(x)$ נובע כי $r_n < r_m$, $r_n < \alpha$ עבור n זוגי ו-$r_n > r_m$, $r_n > \alpha$ עבור n אי-זוגי.

■

למה 4. ההפרש $r_n - r_{n+1}$ שואף ל-0.

הוכחה. מנוסחא (15) נובע

$$\left|r_n - r_{n+1}\right| = \left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| = \left|\frac{p_n q_{n+1} - p_{n+1} q_n}{q_n q_{n+1}}\right| = \left|\frac{1}{q_n q_{n+1}}\right| \le \frac{1}{q_n^{\ 2}} \qquad (17)$$

עכשיו הלמה נובעת מהמסקנה הבאה של נוסחא (14): סדרה q_n עולה בצורה לא חסומה. $\blacksquare$

משפט 3. סדרה r_n מתכנסת למספר α.

הוכחה. לפי למה 3 תת-סדרה עם אינדקסים אי-זוגיים מונוטונית עולה וחסומה מלעיל (למשל, על ידי α או על ידי כל איבר של סדרה עם אינדקס אי-זוגי). לפי משפט בולצנו-ויירשטרס, היא מתכנסת למספר קטן או שווה ל-α. באופן דומה תת-סדרה עם אינדקסים זוגיים מונוטונית יורדת וחסמה מלרע, לכן היא מתכנסת למספר גדול או שווה ל-α. לפי למה 4 הפרש של שתי תתי-הסדרות יורד ל-0, ולכן שני הגבולים שווים ל-α. זה אומר כי גבול של r_n שווה ל-α. $\blacksquare$

הערה. בנינו שבר משולב בהינתן מספר α. אבל שבר משולב אינסופי אפשר לבנות מסדרה כלשהי של מספרים חיוביים (חוץ מאולי a_0) ושלמים. הערך של השבר המשולב הינו גבול של סדרת השברים המתקרבים שלו.

שברים מתקרבים כקירוב רציונלי של מספרים ממשים

בגלל ש-α נמצא בין r_n ל-r_{n+1}, מנוסחה (17) נובע $\left|\frac{p_n}{q_n} - \alpha\right| < \frac{1}{q_n^{\ 2}}$. במילים אחרות, השברים המתקרבים של מספר α הינם קירובים טובים שלו. המשפט הבא מראה כי במובן מסויים הטענה נכונה גם בכיוון הפוך: אם מספר רציונלי מקרב את α בצורה טובה, אז הוא מהווה איזשהו שבר מתקרב של α. אבל צריך להגדיר יותר

במדוייק מה זה "מקרב בצורה טובה": מידה "כמה הקירוב טוב" שונה בין הטענה לטענה ההפוכה פי שתיים.

משפט 4. אם שבר מצומצם $\frac{p}{q}$ מקיים $\left|\frac{p}{q}-\alpha\right|<\frac{1}{2q^2}$, אז $\frac{p}{q}$ הינו שבר מתקרב של מספר α.

הוכחה. בהתחלה נתבונן בפונקציה שהוגדרה על ידי נוסחא (16) ונבין איך היא תראה אם נביא אותה לצורה של שבר רגיל. לשם נוחות נחליף אינדקס n ב-$n+1$. מנוסחא (14) מקבלים: $f_{n+1}(a_{n+1})=\frac{p_{n+1}}{q_{n+1}}=\frac{p_n a_{n+1}+p_{n-1}}{q_n a_{n+1}+q_{n-1}}$. בגלל שהמקדמים p_n, p_{n-1}, q_n, q_{n-1} לא תלויים ב-a_{n+1}, אפשר להסתכל על a_{n+1} כעל משתנה, ולכן לכל x:

$$f_{n+1}(x)=\frac{p_n x+p_{n-1}}{q_n x+q_{n-1}} \qquad (18)$$

לא קשה למצוא פונקציה הפוכה ל-$f_{n+1}(x)$ (נסמן אותה $g_{n+1}(x)$):

$$g_n(x)=\frac{p_{n-1}-q_{n-1}x}{q_n x-p_n} \qquad (19)$$

עכשיו נתבונן בפירוק של מספר $\frac{p}{q}$ לשבר משולב סופי מוכלל:

$$\frac{p}{q}=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\ddots+\cfrac{1}{a_n}}}$$

אם $\alpha > \frac{p}{q}$, אז משתי ההצגות האפשריות נבחר את זאת עם n זוגי, ואם $\alpha < \frac{p}{q}$, אז עם n אי-זוגי. יהי $\omega = g_{n+1}(\alpha)$. אז $\alpha = f_{n+1}(\omega)$, בנוסף

$$\omega + \frac{q_{n-1}}{q_n} = \frac{p_{n-1} - \alpha q_{n-1}}{\alpha q_n - p_n} + \frac{q_{n-1}}{q_n} = \frac{(-1)^n}{q_n{}^2(\alpha - \frac{p_n}{q_n})} = \frac{1}{q^2\left|\alpha - \frac{p}{q}\right|} > 2$$

השתמשנו בנוסחא (15) ושוויון $\frac{p_n}{q_n} = \frac{p}{q}$. מכאן נקבל: $\omega > 2 - \frac{q_{n-1}}{q_n} \geq 1$.

בסוף, נתבונן במספר

$$\alpha' = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n + \cfrac{1}{\omega}}}}$$

בגלל ש-$\omega > 1$, אז $a_0, a_1, \ldots a_n$ - איברים ראשונים של שבר משולב עבור מספר α' (כי הראנו שהצגה של כל מספר בצורה (11) היא יחידה). זאת אומרת ש-$\alpha' = f_{n+1}(\omega)$. מצד שני, בחרנו ω כך ש-$\alpha = f_{n+1}(\omega)$. לכן $\alpha = \alpha'$. ומכאן נובע כי $\frac{p}{q}$ - שבר מתקרב של α. ■

11. שאלה לבדיקת הבנה. בהוכחה הנ"ל יש פאר מסויים: אם α לא שייך לתחום הגדרה של פונקציה g_{n+1}, אז מספר ω לא מוגדר. תשלימו את הפאר הזה.

מידע נוסף על שברים משולבים אפשר למצוא בספרים [1], [3] ו-[5].

פתרון של משוואת פל – מונה ומחנה של שבר מתקרב

משפט 5. יהי (x, y) פתרון חיובי של משוואת פל. אזי (x, y) הינו שבר מתקרב של מספר $\sqrt{m}$.

הוכחה. בגלל ש-$x > y > 0$ ו-$\sqrt{m} > 1$, $x + y\sqrt{m} > 2y$. לכן

$$1 = x^2 - my^2 = (x - y\sqrt{m})(x + y\sqrt{m}) > (x - y\sqrt{m}) \cdot 2y$$

נחלק את השוויון שקיבלנו ב-$2y^2$: $\frac{x}{y} - \sqrt{m} = \frac{1}{2y^2}$. בגלל ש-$(x, y)$ הינו פתרון חיובי של משוואת פל, החלק השמאלי של הביטוי הינו חיובי והשבר $\frac{x}{y}$ מצומצם. לכן, ממשפט 4, היא שבר מתקרב של מספר $\sqrt{m}$. ■

לסיכום, פתרונות חיוביים של משוואות פל צריך לחפש רק בין הזהוגות שמורכבות ממונה ומחנה של שבר מתקרב של $\sqrt{m}$. נשאלת השאלה, אילו בדיוק מהשברים המתקרבים הינם פתרונות של המשוואה. משפט 6 נותן תשובה לשאלה זאת. נביא את המשפט ללא הוכחה. בניסוח של המשפט משתמשים בעובדה שאיברי שבר משולב עבור מספר $\sqrt{m}$ מהווים סדרה מחזורית (ראה הערה לשאלה 8).

משפט 6. יהי n - אורך המחזור של שבר משולב עבור מספר $\sqrt{m}$. מונה ומחנה של שבר מתקרב של מספר $\sqrt{m}$ הינם פתרון למשוואת פל אם ורק אם לאינדקס שלה יש צורה $kn - 1$ (כלומר שווה ל--1 מודולו n) ואי-זוגי.

הוכחה של המשפט, וגם עובדות מעניינות נוספות מתורת המספרים תוכלו למצוא בספר [3]. על משוואות פל ועל משוואות דיאופנטיות אחרות אפשר לקרוא גם בספרים [4] ו-[6].

שיטת השברים המשולבים הינה מספיק יעילה בשביל חיפוש פתרונות למשוואות פל. למשל, במקרה של $m = 61$, שהוא הכי "כבד" לחישוב בין כל הערכים $m < 100$, הפתרון נמצא כבר בצעד 21. חישוב כזה היה אפשרי לביצוע ידני כבר למתמטיקאים בזמנים העתיקים. והיום שימוש במחשב הופך אותו לתרגיל קל. נקבל $x = 1766319049$, $y = 226153980$.

משוואות קשורות למשוואות פל

מצאנו תשובות לשלושת השאלות שנשאלו בתחילת הספר (ראה עמוד 3) לגבי משוואות פל. חובה לציין כי ממש לא לכל משוואות דיאופנטיות יש תשובות כל-כך ממצאות לשאלות כאלה, אפילו אם המשוואות הן פשוטות מאוד. לחילופין, קיום של התשובות זה יותר צירוף מקרים קסום, מאשר כלל.

בתור דוגמא נתבונן במשוואה שדומה מאוד למשוואת פל:

$$x^2 - my^2 = r \qquad (20)$$

כאן החלפנו את 1 בחלק ימין של השוויון במספר שלם כלשהו $r \neq 0$ שונה מ-0.

לפתור משוואה כזאת (קשורה למשוואה פל) זה למצוא כל נקודות שלמות על היפרבולה שרירותית באיור 5 (עמוד 13). ברור כי או שלמשוואה (20) אין פתרון, או שיש לה אינסוף פתרונות. אכן, אם קיים פתרון אחד, אז אם נכפיל אותו בכל הפתרונות של משוואת פל המתאימה, נקבל את כל הפתרונות של המשוואה הקשורה. הם יהיו אינסוף, ותהיה התאמה חד-חד-ערכית ועל בינם לבין פתרונות של משוואת פל מתאימה.

עדיין אין תשובה לשאלה עבור אילו זוגות של m ו-r למשוואה (20) יש לפחות פתרון אחד. בשונה מהמקרה הפרטי של $r = 1$, פתרון כללי לא תמיד קיים. אחד התנאים לקיום של הפתרון ברור: זו השאלה האם אפשר לפתור משוואה $x^2 \equiv r \pmod m$ (במילים אחרות, r אמור להיות *שארית ריבועית* מודולו m). אבל התנאי הזה אינו מספיק. קיימות דוגמאות כאשר r הינו שארית ריבועית מודולו m, אבל למשוואה (20) אין פתרון.

המקרה המעניין ביותר הוא כאשר $r=-1$. אז יש לנו משוואה מהסוג:

$$x^2 - my^2 = -1 \qquad (21)$$

משוואה כזאת נקראת *משוואת פל שלילית*. נניח יש לה פתרון. אז מכל הפתרונות שלה אפשר לבחור את הפתרון החיובי המינימלי.

12. הוכח כי כל הפתרונות החיוביים של המשוואה הינם חזקות אי-זוגיות של הפתרון הבסיסי של המשוואה, וכל הפתרונות החיוביים של משוואת פל המתאימה – חזקות זוגיות שלו.

קל לראות כי משפט 5 נשאר בתוקף גם עבור משוואות פל שליליות. ואת משפט 6 אפשר להרחיב בצורה הבאה:

משפט 6'. יהי n - אורך המחזור של סדרת האיברים של שבר משולב עבור מספר $\sqrt{m}$. מונה ומחנה של שבר מתקרב של $\sqrt{m}$ מהווים פתרון למשוואה

$$\left|x^2 - my^2\right| = 1 \qquad (22)$$

אם ורק אם האינדקס של השבר שווה ל--1 מודולו n. בנוסף, אם האינדקס הוא אי-זוגי, אנחנו מקבלים פתרון של משוואת פל, ואם הוא אי-זוגי, מקבלים פתרון של משוואת פל שלילית.

כתוצאה אנחנו מקבלים כי תנאי הכרחי ומספיק לקיום פתרון של משוואת פל שלילית: אורך מחזור של שבר משולב עבור $\sqrt{m}$ הינו אי-זוגי. נשים לב כי התנאי ההכרחי שהזכרנו קודם (מספר -1 אמור להיות שארית ריבועית מודולו m) שקול לכך שלכל מחלקים ראשוניים אי-זוגיים של m יש צורה $4l+1$, ושתיים נכנס לתוך פרוק של m לראשוניים לא יותר מפעם אחת. הנה כמה ערכים ראשונים של m, עבורם התנאי מתקיים, אך למשוואת פל השלילית אין פתרון: 34, 146, 178, 194, 205, 221.
בסוף הספר הביאנו טבלה של פתרונות חיוביים מינימליים של משוואה (22) עבור m קטנים.

סקירה הסטורית

משוואות שהיום קוראים להם משוואות פל נמצאו כבר בעבודות של מתמטיקאיים של יוון עתיקה והודו עתיקה. בעבודות של מתמטיקאי הודי של מאה XII בשם בְהַסקָרָה יש שיטה לפתרון של משוואות אלה, שנקראת השיטה הציקלית. בפרט, בעזרת השיטה הוא מצא פתרון עבור $m = 61$ (ראה עמוד 32). אבל בזמנים ההם עוד לא היה מדובר על להוכיח שהשיטה תמיד מביא לפתרון.

באמצע מאה XVII מתמטיקאי צרפתי מפורסם פייר פרמא ניסח את הבעיה בצורה כללית. הנה הניסוח שלו מאחד המכתבים:

> *לכל מספר שאינו ריבוע קיים אינסוף ריבועים, שאם נכפול כל אחד מהם במספר ההוא ונוסיף 1, אז התשובה גם תהיה ריבוע.*

פרמא טען כי הוא יודע להוכיח את זה. אבל התוצאה הזאת לא פורסמה, כמו רוב העבודות שלו. לכן ההוכחה של פרמא לא הגיע עד עלינו, ואפילו לא ידוע, האם היא הייתה נכונה.

שני מתמטיקאיים אנגליים, ג'ון ואליס וויליאם בראונקר מצאו דרך נוספת לפתרון של המשוואות, שונה מהשיטה הציקלית. אבל גם הם לא הוכיחו כי השיטה תמיד מביאה לפתרון. יתכן שהם אפילו לא חשבו על זה שהוכחה כזאת נחוצה. ורק בסוף מאה XVIII מתמטיקאי צרפתי ז'וסף לואי לגרנז' הוכיח את הטענה ממכתב של פרמא.

לאונהרד אוילר בטעות כתב שההוכחה שייכת לג'ון פל. מאז למשוואות קוראים על שם פל, למרות שהוא כמעט ולא קשור אליהם. בעצם, טעויות כאלה בהסטוריה של מתמטיקה לא כל-כך נדירות. לפעמים למשוואות פל קוראים גם "משוואות פרמא לא מוגדרות", אך השם "משוואות פל" היום נפוץ הרבה יותר.

בסוף מאה XIX מתמטיקאי ופיזיקאי גרמני מבריק הרמן מינקובסקי פיתח תורה שנקראת גיאומטריית המספרים, בה משתמשים שיטות גיאומטריות עבור פתרון בעיות של תורת המספרים. האובייקטים העיקריים בהם הוא התמקד אלה סריגים מרחביים. בעזרתם מינקובסקי קיבל הרבה תוצאות חדשות בתורת המספרים והוכיח הרבה

משפטים ידועים. בפרט, ההוכחת קיום של פתרון למשוואת פל שהביאנו בספר מבוססת על רעיונות גיאומטריים של מינקובסקי.

אתם יכולים למצוא מידע יותר מפורט על הסטוריה של משוואות פל ועל אלגוריתמים שונים של הפתרון בספר [6].

טבלה של פתרונות חיוביים מינימליים של משוואות $\left|x^2-my^2\right|=1$

בטבלה לכל $m\le 250$ שאינו ריבוע שלם הביאנו פתרון חיובי מינימלי של המשוואה $\left|x^2-my^2\right|=1$. בעמודה השנייה ציינו n - אורך של מחזור של שבר משולב עבור מספר $\sqrt{m}$. בעמודה שלישית יש מספר r שהינו 1 או -1, כתלות בסימן של הביטוי בתוך ערך מוחלט בחלק שמאלי של המשוואה. במקרה של $r=-1$, כדי לקבל פתרון חיובי מינימלי של משוואת פל, צריך מהזוג $(x,\ y)$ ליצור זוג $(x^2+my^2,\ 2xy)$.

m	n	r	x	y
2	1	-1	1	1
3	2	1	2	1
5	1	-1	2	1
6	2	1	5	2
7	4	1	8	3
8	2	1	3	1
10	1	-1	3	1
11	2	1	10	3
12	2	1	7	2
13	5	-1	18	5
14	4	1	15	4
15	2	1	4	1
17	1	-1	4	1
18	2	1	17	4
19	6	1	170	39
20	2	1	9	2
21	6	1	55	12
22	6	1	197	42
23	4	1	24	5
24	2	1	5	1

26	1	-1	5	1
27	2	1	26	5
28	4	1	127	24
29	5	-1	70	13
30	2	1	11	2
31	8	1	1520	273
32	4	1	17	3
33	4	1	23	4
34	4	1	35	6
35	2	1	6	1
37	1	-1	6	1
38	2	1	37	6
39	2	1	25	4
40	2	1	19	3
41	3	-1	32	5
42	2	1	13	2
43	10	1	3482	531
44	8	1	199	30
45	6	1	161	24
46	12	1	24335	3588
47	4	1	48	7
48	2	1	7	1
50	1	-1	7	1
51	2	1	50	7
52	6	1	649	90
53	5	-1	182	25
54	6	1	485	66
55	4	1	89	12
56	2	1	15	2
57	6	1	151	20
58	7	-1	99	13
59	6	1	530	69
60	4	1	31	4
61	11	-1	29718	3805
62	4	1	63	8
63	2	1	8	1
65	1	-1	8	1
66	2	1	65	8
67	10	1	48842	5967
68	2	1	33	4

69	8	1	7775	936
70	6	1	251	30
71	8	1	3480	413
72	2	1	17	2
73	7	-1	1068	125
74	5	-1	43	5
75	4	1	26	3
76	12	1	57799	6630
77	6	1	351	40
78	4	1	53	6
79	4	1	80	9
80	2	1	9	1
82	1	-1	9	1
83	2	1	82	9
84	2	1	55	6
85	5	-1	378	41
86	10	1	10405	1122
87	2	1	28	3
88	6	1	197	21
89	5	-1	500	53
90	2	1	19	2
91	8	1	1574	165
92	8	1	1151	120
93	10	1	12151	1260
94	16	1	2143295	221064
95	4	1	39	4
96	4	1	49	5
97	11	-1	5604	569
98	4	1	99	10
99	2	1	10	1
101	1	-1	10	1
102	2	1	101	10
103	12	1	227528	22419
104	2	1	51	5
105	2	1	41	4
106	9	-1	4005	389
107	6	1	962	93
108	8	1	1351	130
109	15	-1	8890182	851525
110	2	1	21	2

111	6	1	295	28
112	6	1	127	12
113	9	-1	776	73
114	6	1	1025	96
115	10	1	1126	105
116	10	1	9801	910
117	6	1	649	60
118	10	1	306917	28254
119	4	1	120	11
120	2	1	11	1
122	1	-1	11	1
123	2	1	122	11
124	16	1	4620799	414960
125	5	-1	682	61
126	4	1	449	40
127	12	1	4730624	419775
128	4	1	577	51
129	10	1	16855	1484
130	3	-1	57	5
131	6	1	10610	927
132	2	1	23	2
133	16	1	2588599	224460
134	14	1	145925	12606
135	8	1	244	21
136	4	1	35	3
137	9	-1	1744	149
138	4	1	47	4
139	18	1	77563250	6578829
140	4	1	71	6
141	4	1	95	8
142	4	1	143	12
143	2	1	12	1
145	1	-1	12	1
146	2	1	145	12
147	2	1	97	8
148	2	1	73	6
149	9	-1	113582	9305
150	2	1	49	4
151	20	1	1728148040	140634693
152	2	1	37	3

153	8	1	2177	176
154	10	1	21295	1716
155	4	1	249	20
156	2	1	25	2
157	17	-1	4832118	385645
158	8	1	7743	616
159	10	1	1324	105
160	8	1	721	57
161	10	1	11775	928
162	10	1	19601	1540
163	18	1	64080026	5019135
164	6	1	2049	160
165	6	1	1079	84
166	22	1	1700902565	132015642
167	4	1	168	13
168	2	1	13	1
170	1	-1	13	1
171	2	1	170	13
172	16	1	24248647	1848942
173	5	-1	1118	85
174	4	1	1451	110
175	6	1	2024	153
176	4	1	199	15
177	8	1	62423	4692
178	6	1	1601	120
179	14	1	4190210	313191
180	4	1	161	12
181	21	-1	1111225770	82596761
182	2	1	27	2
183	6	1	487	36
184	12	1	24335	1794
185	5	-1	68	5
186	10	1	7501	550
187	6	1	1682	123
188	8	1	4607	336
189	4	1	55	4
190	14	1	52021	3774
191	16	1	8994000	650783
192	4	1	97	7
193	13	-1	1764132	126985

194	4	1	195	14
195	2	1	14	1
197	1	-1	14	1
198	2	1	197	14
199	20	1	16266196520	1153080099
200	2	1	99	7
201	14	1	515095	36332
202	7	-1	3141	221
203	2	1	57	4
204	8	1	4999	350
205	8	1	39689	2772
206	8	1	59535	4148
207	8	1	1151	80
208	6	1	649	45
209	8	1	46551	3220
210	2	1	29	2
211	26	1	278354373650	19162705353
212	14	1	66249	4550
213	12	1	194399	13320
214	26	1	695359189925	47533775646
215	4	1	44	3
216	6	1	485	33
217	16	1	3844063	260952
218	5	-1	251	17
219	4	1	74	5
220	4	1	89	6
221	6	1	1665	112
222	4	1	149	10
223	4	1	224	15
224	2	1	15	1
226	1	-1	15	1
227	2	1	226	15
228	2	1	151	10
229	5	-1	1710	113
230	2	1	91	6
231	2	1	76	5
232	6	1	19603	1287
233	11	-1	23156	1517
234	8	1	5201	340
235	2	1	46	3

236	12	1	561799	36570
237	10	1	228151	14820
238	8	1	11663	756
239	12	1	6195120	400729
240	2	1	31	2
241	17	-1	71011068	4574225
242	10	1	19601	1260
243	10	1	70226	4505
244	26	1	1766319049	113076990
245	10	1	51841	3312
246	10	1	88805	5662
247	12	1	85292	5427
248	4	1	63	4
249	16	1	8553815	542076
250	7	-1	4443	281

ספרות

[1] В. И Арнольд, Цепные дроби. – (серия «Библиотека "Математическое просвещение"», вып. 14) – М. : МЦНМО. 2009. (In Russian).

[2] Z. I. Borevich, I. R. Shafarevich. Number theory. Academic Press. 1966. (Originally published in Russian).

[3] Davenport, H. The Higher Arithmetic. Cambridge University Press. 1982.

[4] Gelfond A.O. The solution of equations in integers. Freeman. 1961. (Originally published in Russian).

[5] A.Ya. Khinchin. Continued Fractions. University of Chicago Press. 1964. (Originally published in Russian).

[6] H. M. Edwards. Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory. Springer. 2000.

תשובות, פתרונות והערות לתרגילים

1. ללא הגבלת הכלליות נניח $m > n$. מהשוויון

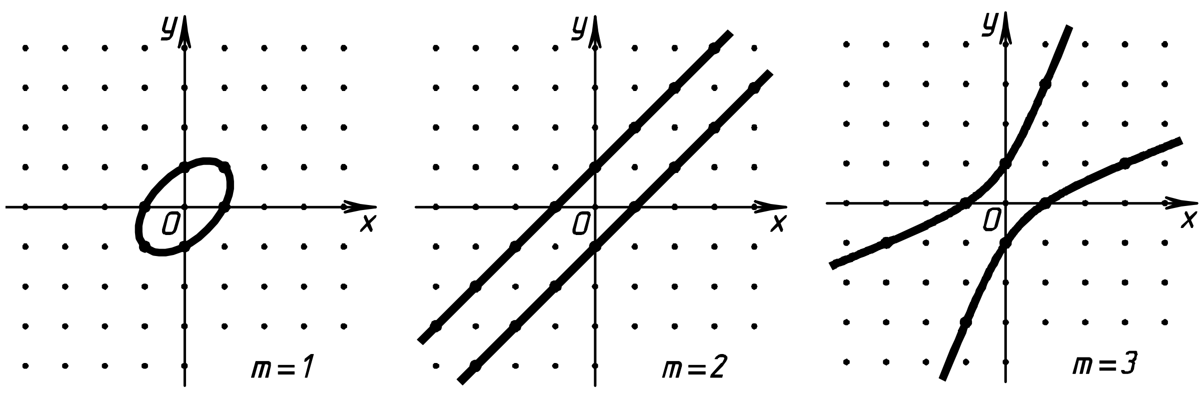
$$2^{2^m}+1=(2^{2^n}-1)(2^{2^n}+1)(2^{2^n}+1)\cdot\ldots\cdot(2^{2^n}+1)+2$$

נובע כי שארית של חלוקת מספר $2^{2^m}+1$ במספר $2^{2^n}+1$ שווה ל-2. לכן

$$\gcd(2^{2^m}+1,\ 2^{2^n}+1)=\gcd(2^{2^n}+1,\ 2)=1.$$

2. על האסימפטוטה $x=y\sqrt{m}$ מופעלת הומותטיה עם מקדם $x_0+y_0\sqrt{m}$. כתוצאה מכך כל הנקודות של האסימפטוטה מתרחקות מראשית הצירים. באופן דומה, על האסימפטוטה $x=-y\sqrt{m}$ מופעלת הומותתיה עם מקדם $x_0-y_0\sqrt{m}$, וכל הנקודות שלה מתקרבות לראשית הצירים. ראשית הצירים עצמה (נקודת חיתוך של האסימפטוטות) הינה נקודה יחידה שנשארת במקום.

3. לגרף של המשוואה הנ"ל יש שלוש אפשרויות: אליפסה (כאשר $m=1$), זוג קווים מקבילים ($m=2$), או היפרבולה ($m\geq 3$). ראה את הגרפים עבור $m=1,\ 2,\ 3$ באיור 13.

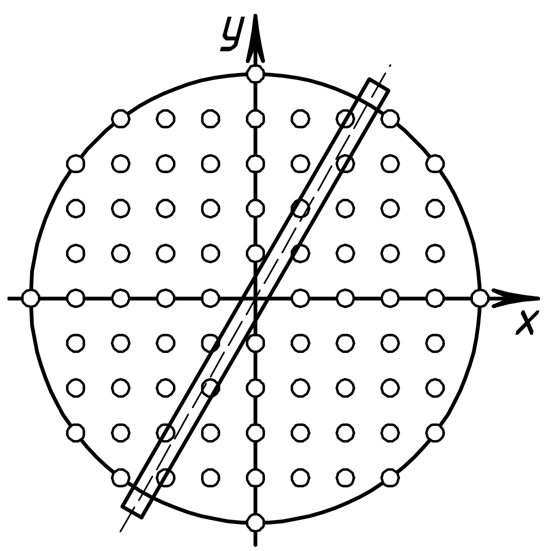


איור 13

נתבונן בשתי טרנספורמציות של מישור המוגדרות על ידי הנוסחאות $f(x,\ y)=(y,\ my-x)$ ו- $g(x,\ y)=(mx-y,\ x)$. אפשר לבדוק כי כל אחת מהטרנספורמציות מעבירה פתרון של המשוואה לפתרון נוסף, וגם הן הפוכות אחת

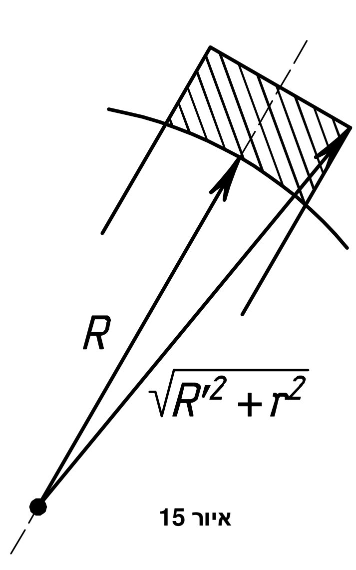
לשנייה. בפרט, זה אומר כי זוגות $(\varphi_k,\ \varphi_{k+1})$ הינם פתרונות של המשוואה. נראה כי פתרונות שמקיימים: $0 \le x < y$ הם כולם מהצורה הזאת. נניח בשלילה כי יש פתרון נוסף, והוא נמצא על הגרף בין שני פתרונות: $(\varphi_{k-1},\ \varphi_k)$ ו-$(\varphi_k,\ \varphi_{k+1})$. נפעיל עליו טרנספורמציה g^k ונקבל פתרון שנמצא בין $(-1,\ 0)$ ל-$(0,\ 1)$. מקבלים סתירה, כי בתחום הזה אין פתרונות.

4. ניקח בתור יחידת מדידה את מטר שהוא המרחק בין העצים הסמוכים. נסמן רדיוס של הגן ב-$R = 1000$, ורדיוס של עץ אחד ב-$r = 0.001$.



איור 14

נבחר כיוון מסויים. נסמן ב-R' "מספר קצת יותר גדול מ-R" – בהמשך נפרט על זה. נבנה מלבן שמרכזו מתלכד עם מרכז הגן, כך שאחת הצלעות שלו מקבילה לכיוון שבחרנו ואורכה $2R'$, ואורכה של הצלע השנייה שווה ל- $2r$ (ראה איור 14). שטחו של המלבן שווה ל-$4R'r$ ומתקיים $4R'r > 4Rr = 4$. מלמת מינקובסקי, בתוך המלבן יש קודקוד של הרשת שיסתיר את תצפית בכיוון שבחרנו.



איור 15

נותר להוכיח כי הקודקוד הנ"ל לא נמצא מחוץ לגן. בשביל זה נתבונן בחלק של המלבן ששנמצא מחוץ למעגל ברדיוס R (ראה איור 15). ריבוע של מרחק מכל נקודה בתחום זה עד מרכז הגן גדול מ-R^2 ולא עובר את $R'^2 + r^2$. אפשר לבחור R' מספיק קטן, כך שיתקיים $R'^2 + r^2 < R^2 + 1$. לכן ריבוע של מרחק מנקודה כלשהי בתחום עד מרכז המעגל הוא שבר. אבל ריבוע של מרחק בין כל שתי נקודות שלמות זה מספר שלם. לכן בתחום זה אין נקודות שלמות.

5. נתבונן בעקום שמוגדר על ידי המשוואה $ax^2+2bxy+cy^2=\lambda^2$, כאשר $\frac{4}{\pi}<\lambda^2<2$. העקום הזה הוא אליפסה שחצאי צירים שלה שווים ל-

$$d_{1,2}=\frac{\lambda}{\sqrt{\frac{a+c\pm\sqrt{(a+c)^2-4}}{2}}}$$

שטח של האליפסה שווה ל-$\pi d_1 d_2=\pi\lambda^2>4$. מלמת מינקובסקי, בתוך האליפסה יש נקודה שלמה $(x_0,\, y_0)$ ששונה מראשית הצירים. ערך של ${ax_0}^2+2bx_0y_0+c{y_0}^2$ אמור להיות שלם, חיובי וקטן מ-λ^2, לכן הוא שווה ל-1.

6. אם m הוא ריבוע שלם, אז קיימות נקודות שלמות שונות מראשית הצירים שנמצאות על אסימפטוטות של היפרבולות. למרות זאת, בסיום של ההוכחה השתמשנו בעובדה שכל הנקודות השלמות חוץ מראשית הצירים נמצאות (ממש) בתוך אחת מארבעת הזוויות שנוצרות על ידי האסימפטוטות.

7. אם שבר משולב הוא סופי, אפשר להפוך אותו לשבר רגל, שזה שקול למספר רציונלי.

בכיוון הפוך, יהי מספר רציונלי α כך ש-$\alpha=a_0+\frac{1}{\alpha_1}$, a_0 – מספר שלם, $\alpha_1>1$.

אזי אם $\alpha=\frac{p}{q}$, אז a_0 היא מנה של חילוק של p ב-q, ו-$\alpha_1=\frac{q}{r}$, כאשר r היא שארית של חילוק של p ב-q. לכן סדרת α_i מורכבת ממספרים רציונליים שסדרת המחנים שלהם יורדת. לכן סדרה α_i היא סופית.

8. אם סדרת a_n הינה מחזורית, אז קיימים אינדקסים k ו- l כך ש- $a_k = a_l$. מכאן $g_k(\alpha) = g_l(\alpha)$, כאשר g_k ו- g_l הן הפונקציות הרציונליות המוגדרות על ידי נוסחאות (19). אחרי זה מביאים את המשוואה שקיבלנו לצורה סטנדרטית של משוואה ריבועית.

9. בסיס האינדוקציה. בדיקה ישירה ששוויונים (14) מתקיימים עבור $n=1$.
צעד האינדוקציה. לפי הנחת אינדוקציה, עבור $n \geq 2$ מתקיים:

$$\frac{p_n}{q_n} = \frac{p_{n-1}a_n + p_{n-2}}{q_{n-1}a_n + q_{n-2}}.$$

אם נציב לחלק הימני של השוויון $a_n + \frac{1}{a_{n+1}}$ במקום a_n, נקבל $\frac{p_{n+1}}{q_{n+1}}$. לכן,

$$\frac{p_{n+1}}{q_{n+1}} = \frac{p_{n-1}\left(a_n + \frac{1}{a_{n+1}}\right) + p_{n-2}}{q_{n-1}\left(a_n + \frac{1}{a_{n+1}}\right) + q_{n-2}} = \frac{p_{n-1}a_n + p_{n-2} + \frac{p_{n-1}}{a_{n+1}}}{q_{n-1}a_n + q_{n-2} + \frac{q_{n-1}}{a_{n+1}}} = \frac{p_n a_{n+1} + p_{n-1}}{q_n a_{n+1} + q_{n-1}}$$

הוכחנו כי השברים $\frac{p_n}{q_n}$ שמקבלים מנוסחאות נסיגה (14) שוות לשברים המתקרבים. נשאר להוכיח כי השברים האלה מצומצמים. זה נובע מפתרון של שאלה 10 שמופיע בהמשך (מותר להשתמש בו כאן, כי ההוכחה שם לא משתמשת בזה ש- p_n ו- q_n זרים). אם נניח של- p_n ו- q_n יש מחלק משותף, אז הוא חייב לחלק גם את מספר $p_{n-1}q_n - p_n q_{n-1} = (-1)^n$. לכן המחלק המשופת ההיחיד שלהם זה 1.

10. בסיס האינדוקציה. בדיקה ישירה של מקרה $n=1$:
מציבים $p_0 = a_0,\ q_0 = 1,\ p_1 = a_0a_1 + 1,\ q_1 = a_1$.
נכפיל את הנוסחא הראשונה מ-(14) ב- q_n, ואת הנוסחא הראשונה ב- p_n ונחסר אותן. נקבל $p_n q_{n+1} - p_{n+1}q_n = -(p_{n-1}q_n - p_n q_{n-1})$. מכאן נובע צעד האינדוקציה.

11.פונקציה $g_{n+1}(x)$ מוגדרת רק עבור $x = \frac{p_n}{q_n}$. אבל אם $\alpha = \frac{p}{q}$, אז רואים כי הטענה של המשפט בהחלט נכונה.

12.יהי $(x_0,\ y_0)$ – הפתרון החיובי המינימלי של משוואה (22). (משמעות של "מינימלי" כאן זה שערך של הביטוי $x_0 + y_0\sqrt{m}$ הוא מינימלי.) אזי כל הפתרונות של המשוואה הם חזקות של הפתרון המינימלי. אכן, יהי $(x,\ y)$ – פתרון חיובי שרירותי. נסמן $u_0 = x_0 + y_0\sqrt{m},\ u = x + y\sqrt{m}$. אם הפתרון $(x,\ y)$ אינו חזקה של $(x_0,\ y_0)$, אז קיים n שעבורו $u_0^{\,n} < u < u_0^{\,n+1}$. נכפיל את הביטו ב-$u_0^{\,-n}$ ונקבל: $1 < uu_0^{\,-n} < u_0$. נשים לב כי אז קיים פתרון חיובי למשוואה (22) המתאים ל-$uu_0^{\,-n}$, והוא קטן מ-$(x_0,\ y_0)$, בסתירה למינימליות של $(x_0,\ y_0)$.

אם $(x_0,\ y_0)$ הינו פתרון של משוואת פל, אז גם כל החזקות שלו הם פתרונות של המשוואה, ולכן אין למשוואה פתרונות שליליים. לחילופין, אם $(x_0,\ y_0)$ הוא פתרון שלילי, אז החזקות הזוגיות שלו הן פתרונות של משוואת פל, והחזקות השליליות הן הפתרונות השליליים.